config コマンド：j ～ q

config known ap

既知の Cisco Lightweight アクセス ポイントを設定するには、**config known ap** コマンドを使用します。

config known ap {**add** | **alert** | **delete**} *MAC*

構文の説明

add	新しい既知のアクセス ポイント エントリを追加します。
alert	アクセス ポイントの検出時にトラップを生成します。
delete	既存の既知のアクセス ポイント エントリを削除します。
MAC	既知の Cisco Lightweight アクセス ポイントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、新しいアクセス ポイント エントリ ac:10:02:72:2f:bf を既知のアクセス ポイントに追加する例を示します。

```
(Cisco Controller) >config known ap add ac:10:02:72:2f:bf 12
```

config lag

リンク集約（LAG）を有効または無効にするには、**config lag** コマンドを使用します。

config lag {**enable** | **disable**}

構文の説明

enable	リンク集約（LAG）設定を有効にします。
disable	リンク集約（LAG）設定を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、LAG 設定を有効にする例を示します。

```
(Cisco Controller) > config lag enable
Enabling LAG will map your current interfaces setting to LAG interface,
All dynamic AP Manager interfaces and Untagged interfaces will be deleted
All WLANs will be disabled and mapped to Mgmt interface
Are you sure you want to continue? (y/n)
You must now reboot for the settings to take effect.
```

次に、LAG 設定を無効にする例を示します。

```
(Cisco Controller) > config lag disable
Disabling LAG will map all existing interfaces to port 1.
Are you sure you want to continue? (y/n)
You must now reboot for the settings to take effect.
```

config ldap

Lightweight Directory Access Protocol（LDAP）サーバの設定を行うには、**config ldap** コマンドを使用します。

config ldap {**add** | **delete** | **enable** | **disable** | **retransmit-timeout** | **retry** | **user** | **security-mode** | **simple-bind**} *index*

config ldap add *index server_ip_address port user_base user_attr user_type* [**secure**]

config ldap retransmit-timeout *index retransmit-timeout*

config ldap retry *attempts*

config ldap user {**attr** *index user-attr* | **base** *index user-base* | **type***index user-type*}

config ldap security-mode {**enable** | **disable**}*index*

config ldap simple-bind {**anonymous** *index* | **authenticated** *index username password*}

構文の説明

add	LDAP サーバの追加を指定します。
delete	LDAP サーバの削除を指定します。
enable	LDAP サーバの有効化を指定します。
disable	LDAP サーバの無効化を指定します。
retransmit-timeout	LDAP サーバのデフォルト再送信タイムアウトを変更します。
retry	LDAP サーバの再試行回数を設定します。
user	ユーザ検索パラメータを設定します。
security-mode	セキュリティ モードを設定します。
simple-bind	ローカル認証バインド方式を設定します。
anonymous	LDAPサーバへの匿名アクセスを許可します。
authenticated	LDAP サーバに安全にアクセスのため、ユーザ名とパスワードを入力することを指定します。
index	LDAP サーバインデックス。範囲は 1 ～ 17 です。
server_ip_address	LDAP サーバの IP アドレス。

port	ポート番号。
user_base	すべてのユーザを含むサブツリーの識別名。
user_attr	ユーザ名を含む属性。
user_type	ユーザを識別するオブジェクト タイプ。
secure	（任意）Transport Layer Security（TLS）を使用することを指定します。
retransmit-timeout	LDAP サーバの再送信タイムアウト。指定できる範囲は 2 ～ 30 です。
attempts	各 LDAP サーバを再試行する回数。
attr	ユーザ名を含む属性を設定します。
base	すべてのユーザを含むサブツリーの識別名を設定します。
type	ユーザ タイプを設定します。
username	認証されたバインド方式のユーザ名。
password	認証されたバインド方式のパスワード。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。
7.6	セキュア LDAP をサポートするために **secure** キーワードが追加されました。

使用上のガイドライン

セキュア LDAP を有効にすると、コントローラはサーバ証明書を検証しなくなります。

次に、LDAP サーバ インデックス 10 を有効にする例を示します。

```
(Cisco Controller) > config ldap enable 10
```

関連コマンド

config ldap add

config ldap simple-bind

show ldap summary

config local-auth active-timeout

設定済みのRADIUSサーバのペアによる認証が失敗した後に、コントローラがローカル拡張認証プロトコル（EAP）を使用してワイヤレスクライアントの認証を試行する時間を指定するには、**config local-auth active-timeout** コマンドを使用します。

config local-auth active-timeout *timeout*

構文の説明

timeout	タイムアウト時間を秒単位で指定します。有効な範囲は 1 ～ 3600 です。

コマンド デフォルト

デフォルトのタイムアウト値は 100 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、EAPを使用して、ワイヤレスクライアントを認証するためのアクティブタイムアウトを 500 秒に指定する例を示します。

```
(Cisco Controller) > config local-auth active-timeout 500
```

関連コマンド

clear stats local-auth

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config local-auth eap-profile

ローカル拡張可能認証プロトコル（EAP）認証プロファイルを設定するには、**config local-auth eap-profile** コマンドを使用します。

config local-auth eap-profile {[**add** | **delete**] *profile_name* | **cert-issuer** {**cisco** | **vendor**} | **method** *method* **local-cert** {**enable** | **disable**} *profile_name* | **method** *method* **client-cert** {**enable** | **disable**} *profile_name* | **method** *method* **peer-verify ca-issuer** {**enable** | **disable**} | **method** *method* **peer-verify cn-verify** {**enable** | **disable**} | **method** *method* **peer-verify date-valid** {**enable** | **disable**}

構文の説明

add	（任意）EAP プロファイルまたは方式の追加を指定します。
delete	（任意）EAP プロファイルまたは方式の削除を指定します。
profile_name	EAP プロファイル名（最大 63 文字の英数字）。プロファイル名にはスペースは使用できません。
cert-issuer	（Extensible Authentication Protocol Transport Layer Security（EAP-TLS）、Protected Extensible Authentication Protocol（PEAP）、または Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）と証明書を使用している場合）クライアントに送信される証明書の発行元を指定します。証明書発行元としてはCiscoまたはサードパーティ ベンダーがサポートされています。
cisco	シスコの証明書の発行元を指定します。
vendor	サード パーティ ベンダーを指定します。
method	EAP プロファイル方式を設定します。
method	EAP プロファイル方式名。サポートされている方式は leap、fast、tls、および peap です。
local-cert	（EAP-FASTで使用する場合）認証のために、コントローラ上にデバイス証明書が必要かどうかを指定します。
enable	パラメータ ID の有効化を指定します。
disable	パラメータ ID の無効化を指定します。

client-cert	（EAP-FAST で使用する場合）認証用のデバイス証明書をコントローラへ送信するために、無線クライアントが必要かどうかを指定します。
peer-verify	ピア証明書検証オプションを設定します。
ca-issuer	（EAP-TLS または EAP-FAST と証明書を使用している場合）クライアントから受信した証明書を、コントローラ上の認証局（CA）の証明書と照合するかどうかを指定します。
cn-verify	（EAP-TLS または EAP-FAST と証明書を使用している場合）受信した証明書の通常名（CN）をコントローラ上の CA 証明書の CN と照合するかどうかを指定します。
date-valid	（EAP-TLS または EAP-FAST と証明書を使用している場合）受信したデバイス証明書が有効で期限切れになっていないことをコントローラで検証するかどうかを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FAST01 という名前のローカル EAP プロファイルを作成する例を示します。

```
(Cisco Controller) > config local-auth eap-profile add FAST01
```

次に、ローカル EAP プロファイルに EAP-FAST 方式を追加する例を示します。

```
(Cisco Controller) > config local-auth eap-profile method add fast FAST01
```

次に、EAP-FAST プロファイルのクライアントに送信される証明書の発行元としてシスコを指定する例を示します。

```
(Cisco Controller) > config local-auth eap-profile method fast cert-issuer cisco
```

次に、クライアントから受信する証明書がコントローラ上の CA 証明書と照合されるように指定する例を示します。

```
(Cisco Controller) > config local-auth eap-profile method fast peer-verify ca-issuer
enable
```

関連コマンド

config local-auth active-timeout

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config local-auth method fast

EAP-FAST プロファイルを設定するには、**config local-auth method fast** コマンドを使用します。

config local-auth method fast {**anon-prov** [**enable** | **disable**] | **authority-id** *auth_id* **pac-ttl** *days* | **server-key** *key_value*}

構文の説明

anon-prov	匿名プロビジョニングが可能なようにコントローラを設定します。これにより、Protected Access Credential（PAC）プロビジョニング中に、PAC を持たないクライアントに PAC を自動的に送信できるようになります。
enable	（任意）パラメータを有効化することを指定します。
disable	（任意）パラメータを無効化することを指定します。
authority-id	ローカル EAP-FAST サーバの権限識別子を設定します。
auth_id	ローカル EAP-FAST サーバの権限識別子（2 ～ 32 の 16 進数値）。
pac-ttl	Protected Access Credential（PAC）の有効期間の日数を設定します。これは存続可能時間（TTL）値とも呼ばれます。
days	存続可能時間（TTL）の値（1 ～ 1000 日）。
server-key	PAC を暗号化または復号化するサーバ キーを設定します。
key_value	暗号キーの値（2 ～ 32 の 16 進数値）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、匿名プロビジョニングを許可するためにコントローラを無効にする例を示します。

```
(Cisco Controller) > config local-auth method fast anon-prov disable
```

次に、ローカルEAP-FASTサーバの権限識別子0125631177を設定する例を示します。

```
(Cisco Controller) > config local-auth method fast authority-id 0125631177
```

次に、PACの有効日数を10日に設定する例を示します。

```
(Cisco Controller) > config local-auth method fast pac-ttl 10
```

関連コマンド

clear stats local-auth

config local-auth eap-profile

config local-auth active-timeout

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config local-auth user-credentials

ユーザ クレデンシャルをローカル拡張可能認証プロトコル（EAP）認証データベースで検索する順序を設定するには、**config local-auth user credentials** コマンドを使用します。

config local-auth user-credentials ｛**local**［**ldap**］ | **ldap**［**local**］ ｝

構文の説明

local	ユーザ クレデンシャルをローカル データベースで検索することを指定します。
ldap	（任意）ユーザ クレデンシャルを Lightweight Directory Access Protocol（LDAP）データベースで検索することを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

特定のデータベース パラメータの順序は、データベースの検索順序を示します。

次に、ローカル EAP 認証データベースが検索される順序を指定する例を示します。

```
(Cisco Controller) > config local-auth user credentials local lda
```

上記の例では、最初にローカル データベースが検索され、次に LDAP データベースが検索されます。

関連コマンド

clear stats local-auth

config local-auth eap-profile

config local-auth method fast

config local-auth active-timeout

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config lync-sdn

Lync サービスを設定するには、 **config lync-sdn** コマンドを使用します。

config lync-sdn {**port** *port-number*} | {**enable** | **disable**}

構文の説明

port	Lync サーバ ポート番号を設定します。
port-number	サーバのポート番号。
enable	Lync サービスをグローバルに有効にします。
disable	Lync サービスをグローバルに無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、Lync サービスをグローバルに有効にする例を示します。

```
(Cisco Controller) >config lync-sdn enable
```

config licensing

シスコ スマート ソフトウェア ライセンシングと RTU ライセンス プラットフォームを切り替えるには、**config licensing** コマンドを使用します。

config licensing {**rtu** | **smart-license**} **dns-server** *ip address*

構文の説明

rtu	使用権（RTU）ライセンスプラットフォーム。
smart-license	シスコ スマート ソフトウェア ライセンシング。
dns-server	スマート ソフトウェア ライセンシングの DNS サーバ パラメータを設定します。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

コマンド デフォルト

使用権（RTU）が、デバイスのデフォルトのライセンス メカニズムです。

次に、コントローラでシスコ スマート ソフトウェア ライセンシングをアクティブにする例を示します。

```
(Cisco Controller) > config licensing smart-license dns-server 209.165.200.224
```

（注） ライセンス プラットフォームの変更をアクティブにするにはコントローラを再起動する必要があります。

config license boot

Cisco 5500 シリーズのコントローラの次回リブート時に使用するライセンス レベルを指定するには、**config license boot** コマンドを使用します。

config license boot {**base** | **wplus** | **auto**}

構文の説明

base	base ブート レベルを指定します。
wplus	wplus ブート レベルを指定します。
auto	auto ブート レベルを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

auto を入力すると、ライセンス ソフトウェアは、次回リブート時に使用するライセンス レベルを自動的に選択します。通常、評価ライセンスよりも永久ライセンスのほうが優先されます。また、ベース ライセンスよりも WPLUS ライセンスのほうが優先されます。

（注） ベース ライセンスから WPLUS ライセンスへのアップグレードを検討している場合、WPLUS 評価ライセンスを試してから WPLUS 永久ライセンスにアップグレードできます。評価ライセンスをアクティブ化するには、ベース永久ライセンスではなく WPLUS 評価ライセンスがコントローラで使用されるように、イメージ レベルを設定する必要があります。

（注） 操作の中断を避けるために、コントローラは、評価ライセンスの有効期限が切れてもライセンスを切り替えません。永久ライセンスに戻すには、コントローラをリブートする必要があります。リブート後に、期限切れになった評価ライセンスと同じフィーチャ セット レベルにコントローラがデフォルト設定されます。同じフィーチャ セット レベルの永久ライセンスがインストールされていない場合、コントローラは、別のレベルの永久ライセンスまたは有効期限の切れていない評価ライセンスを使用します。

次に、ライセンスのブート設定を wplus に設定する例を示します。

```
(Cisco Controller) > config license boot wplus
```

関連コマンド

license install

show license in-use

license modify priority

config load-balancing

アグレッシブなロード バランシングをコントローラでグローバルに設定するには、**config load-balancing** コマンドを使用します。

config load-balancing {**window** *client_count* | **status** {**enable** | **disable**} | **denial** *denial_count*}

config load-balancing uplink-threshold *traffic_threshold*

構文の説明

window	アグレッシブなロードバランシング クライアント ウィンドウを指定します。
client_count	1 ～ 20 のクライアントを含む、アグレッシブなロードバランシング クライアント ウィンドウ。
status	ロード バランシングの状態を設定します。
enable	ロード バランシング機能をイネーブルにします。
disable	ロード バランシング機能をディセーブルにします。
denial	ロードバランシング時に拒否されるアソシエーションの数を指定します。
denial_count	ロード バランシング中のアソシエーション拒否の最大数（0 ～ 10）。
uplink-threshold	アクセス ポイントが新しいアソシエーションを拒否できるように、しきい値のトラフィックを指定します。
traffic_threshold	アクセス ポイントが新しいアソシエーションを拒否するためのしきい値のトラフィック。この値は、90 秒間隔で測定された WAN 使用率のパーセントです。たとえば、デフォルトしきい値が 50 である場合、アクセス ポイント WAN インターフェイスで 50% 以上の使用率が検出されると、ロード バランシングがトリガされます。

コマンド デフォルト

デフォルトでは、アグレッシブなロード バランシングは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

負荷分散が有効になっている WLAN は、音声およびビデオなどの時間依存型アプリケーションをサポートしません。これは、ローミングでの遅延が存在するためです。

コントローラとともに Cisco 7921 および 7920 Wireless IP Phone を使用する場合、各コントローラの音声 WLAN でアグレッシブなロードバランシングが無効化されていることを確認します。無効化されていない場合、電話による初期ローミングが失敗し、オーディオパスが中断されることがあります。

クライアントをロードバランシングできるのは、同じコントローラに接続されているアクセスポイントのみです。WAN 使用率は次の式を使用してパーセントとして産出されます: (送信されたデータ レート (1 秒あたり) + 受信したデータ レート (1 秒あたり))/(1000Mbps TX + 1000Mbps RX) * 100

次に、アグレッシブなロード バランシングの設定を有効にする例を示します。

```
(Cisco Controller) > config load-balancing aggressive enable
```

関連コマンド

show load-balancing

config wlan load-balance

config location

ロケーションベースのシステムを設定するには、**config location** コマンドを指定します。

config location {**algorithm** {**simple** | **rssi-average**} | {**rssi-half-life** | **expiry**} [**client** | **calibrating-client** | **tags** | **rogue-aps**] *seconds* | **notify-threshold** [**client** | **tags** | **rogue-aps**] *threshold* | **interface-mapping** {**add** | **delete**} *location wlan_id interface_name* | **plm** {**client** {**enable** | **disable**} *burst_interval* | **calibrating** {**enable** | **disable**} {**uniband** | **multiband**}}}

構文の説明

algorithm	（注） **config location algorithm** コマンドは使用も変更もしないでください。このコマンドは、最適なデフォルト値に設定されています。 平均 RSSI および SNR 値に使用されるアルゴリズムを設定します。
simple	必要とする CPU オーバーヘッドは小さいが精度が低い、高速アルゴリズムを指定します。
rssi-average	より正確なアルゴリズムが指定されますが、より多くの CPU オーバーヘッドが必要です。
rssi-half-life	（注） **config location rssi-half-life** コマンドは使用も変更もしないでください。このコマンドは、最適なデフォルト値に設定されています。 2 つの RSSI 測定値を平均するときに、半減期を設定します。
expiry	（注） **config location expiry** コマンドは使用も変更もしないでください。このコマンドは、最適なデフォルト値に設定されています。 RSSI 値のタイムアウトを設定します。
client	（任意）クライアント デバイスに適用するパラメータを指定します。
calibrating-client	（任意）調整クライアント デバイスに使用するパラメータを指定します。
tags	（任意）無線周波数ID（RFID）タグに適用するパラメータを指定します。

rogue-aps	（任意）不正なアクセス ポイントに適用するパラメータを指定します。
seconds	秒数を指定します（0、1、2、5、10、20、30、60、90、120、180、300 秒）。
notify-threshold	（注） **config location notify-threshold** コマンドは使用も変更もしないでください。このコマンドは、最適なデフォルト値に設定されています。 RSSI 測定に NMSP 通知しきい値を指定します。
threshold	しきい値のパラメータ。範囲は 0 ～ 10 dB で、デフォルト値は 0 dB です。
interface-mapping	新規のロケーション、無線 LAN、またはインターフェイス マッピング要素を追加または削除します。
wlan_id	WLAN の識別名。
interface_name	マッピング要素を適用するインターフェイスの名前。
plm	通常のクライアントまたは調整クライアントのパス損失測定（S60）要求を指定します。
client	通常の、未調整のクライアントを指定します。
burst_interval	バースト間隔。有効範囲は 1 ～ 3600 秒で、デフォルト値は 60 秒です。
calibrating	調整クライアントを指定します。
uniband	関連付けられた 802.11a または 802.11b/g 無線を指定します（ユニバンド）。
multiband	関連付けられた 802.11a/b/g 無線を指定します（マルチバンド）。

コマンド デフォルト

個々の引数およびキーワードのデフォルト値については、「構文の説明」の項を参照してください。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ロケーション ベースのコントローラで RSSI 値および SNR 値を平均する単純なアルゴリズムを指定する例を示します。

```
(Cisco Controller) > config location algorithm simple
```

関連コマンド

config location info rogue

clear location rfid

clear location statistics rfid

show location

show location statistics rfid

config location info rogue

不正サービスの情報通知を設定するには、**config location info rogue** コマンドを使用します。

config location info rogue {**basic** | **extended**}

構文の説明

basic	不正情報通知サービスの基本不正パラメータ（mode、class、containmentlevel、numclients、firsttime、lasttime、ssid など）を設定します。 （注） Cisco MSE のバージョンが Cisco WLC のバージョンより古い場合は、基本パラメータを設定してください。
extended	不正情報通知サービスの拡張不正パラメータ（基本パラメータに加えて、セキュリティ タイプ、LRAD タイプ検出など）を設定します。

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

config logging buffered

コントローラ バッファへのロギング メッセージの重大度を設定するには、**config logging buffered** コマンドを使用します。

config logging buffered security_level

構文の説明

security_level	セキュリティ レベル。次のいずれかを選択します。 • 緊急：重大度 0 • アラート：重大度 1 • 重要：重大度 2 • エラー：重大度 3 • 警告：重大度 4 • 通知：重大度 5 • 情報：重大度 6 • デバッグ：重大度 7

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ロギング メッセージに対するコントローラのバッファの重大度を 4 に設定する例を示します。

```
(Cisco Controller) > config logging buffered 4
```

関連コマンド

config logging syslog facility

config logging syslog level

show logging

config logging console

コントローラ コンソールへのロギング メッセージの重大度を設定するには、**config logging console** コマンドを使用します。

config logging console *security_level*

構文の説明

security_level	重大度。次のいずれかを選択します。 • 緊急：重大度 0 • アラート：重大度 1 • 重要：重大度 2 • エラー：重大度 3 • 警告：重大度 4 • 通知：重大度 5 • 情報：重大度 6 • デバッグ：重大度 7

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ロギング メッセージに対するコントローラのコンソールの重大度を 3 に設定する例を示します。

```
(Cisco Controller) > config logging console 3
```

関連コマンド

config logging syslog facility

config logging syslog level

show logging

config logging debug

デバッグ メッセージをコントローラ バッファ、コントローラ コンソール、または syslog サーバに保存するには、**config logging debug** コマンドを使用します。

config logging debug {**buffered** | **console** | **syslog**} {**enable** | **disable**}

構文の説明

buffered	コントローラ バッファにデバッグ メッセージを保存します。
console	コントローラ コンソールにデバッグ メッセージを保存します。
syslog	syslog サーバにデバッグ メッセージを保存します。
enable	デバッグ メッセージのロギングをイネーブルにします。
disable	デバッグ メッセージのロギングをディセーブルにします。

コマンド デフォルト

デフォルトでは、 **console** コマンドが有効になっており、 **buffered** コマンドと **syslog** コマンドが無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コントローラ コンソールにデバッグ メッセージを保存する例を示します。

```
(Cisco Controller) > config logging debug console enable
```

関連コマンド

show logging

config logging fileinfo

コントローラがメッセージ ログ内にソース ファイルの情報を含めるようにする、またはこの情報を表示しないようにするには、**config logging fileinfo** コマンドを使用します。

config logging fileinfo {**enable** | **disable**}

構文の説明

enable	メッセージログにソース ファイルの情報を含めます。
disable	コントローラがメッセージログのソース ファイルの情報を表示しないようにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コントローラがメッセージログにソース ファイルの情報を含めるようにする例を示します。

```
(Cisco Controller) > config logging fileinfo enable
```

関連コマンド

show logging

config logging procinfo

コントローラがメッセージログ内にプロセス情報を含めるようにする、またはこの情報を表示しないようにするには、**config logging procinfo** コマンドを使用します。

config logging procinfo {**enable** | **disable**}

構文の説明

enable	プロセス情報をメッセージ ログに含めます。
disable	コントローラがメッセージ ログにプロセス情報を表示しないようにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コントローラがメッセージ ログにプロセス情報を含めるようにする例を示します。

```
(Cisco Controller) > config logging procinfo enable
```

関連コマンド

show logging

config logging traceinfo

コントローラがメッセージログ内にトレースバック情報を含めるようにする、またはこの情報を表示しないようにするには、**config logging traceinfo** コマンドを使用します。

config logging traceinfo {**enable** | **disable**}

構文の説明

enable	トレースバック情報をメッセージ ログに含めます。
disable	コントローラがメッセージログにトレースバック情報を表示しないようにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コントローラがメッセージ ログにトレースバック情報を含めないようにする例を示します。

```
(Cisco Controller) > config logging traceinfo disable
```

関連コマンド

show logging

config logging syslog host

syslog メッセージを送信するためにリモート ホストを設定するには、**config logging syslog host** コマンドを使用します。

config logging syslog host *ip_addr*

構文の説明

ip_addr	リモート ホストの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

使用上のガイドライン

- syslog メッセージを送信するためにリモート ホストを設定するには、**config logging syslog host** *ip_addr* コマンドを使用します。
- syslog メッセージを送信するように設定されたリモート ホストを削除するには、**config logging syslog host** *ip_addr* **delete** コマンドを使用します。
- コントローラで設定されている syslog サーバを表示するには、**show logging** コマンドを使用します。

次に、syslog メッセージを送信するために 2 つのリモート ホスト（10.92.125.52 と 2001:9:6:40::623）を設定し、コントローラで設定されている syslog サーバを表示する例を示します。

```
(Cisco Controller) > config logging syslog host 10.92.125.52
System logs will be sent to 10.92.125.52 from now on

(Cisco Controller) > config logging syslog host 2001:9:6:40::623
System logs will be sent to 2001:9:6:40::623 from now on

(Cisco Controller) > show logging
Logging to buffer :
- Logging of system messages to buffer :
 - Logging filter level..................... errors
 - Number of system messages logged..... 1316
 - Number of system messages dropped..... 6892
- Logging of debug messages to buffer ..... Disabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Cache of logging  ..... Disabled
- Cache of logging time(mins) ..... 10080
- Number of over cache time log dropped  ..... 0
Logging to console :
```

```
- Logging of system messages to console :
 - Logging filter level..... disabled
 - Number of system messages logged..... 0
 - Number of system messages dropped..... 8243
- Logging of debug messages to console ..... Enabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
Logging to syslog :
- Syslog facility..... local0
- Logging of system messages to console :
 - Logging filter level..... disabled
 - Number of system messages logged..... 0
 - Number of system messages dropped..... 8208
- Logging of debug messages to console ..... Enabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Logging of system messages to syslog :
 - Logging filter level..... errors
 - Number of system messages logged..... 1316
 - Number of system messages dropped..... 6892
- Logging of debug messages to syslog ..... Disabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Number of remote syslog hosts..... 2
- syslog over tls..... Disabled
  - Host 0..... 10.92.125.52
  - Host 1..... 2001:9:6:40::623
  - Host 2.....
Logging of RFC 5424..... Disabled
Logging of Debug messages to file :
- Logging of Debug messages to file..... Disabled
- Number of debug messages logged..... 0
- Number of debug messages dropped..... 0
Logging of traceback..... Enabled
```

次に、syslog メッセージを送信するために設定されている 2 つのリモート ホスト（10.92.125.52 と 2001:9:6:40::623）を削除し、設定されていた syslog サーバがコントローラから削除されたことを表示する例を示します。

```
(Cisco Controller) > config logging syslog host 10.92.125.52 delete
System logs will not be sent to 10.92.125.52 anymore

(Cisco Controller) > config logging syslog host 2001:9:6:40::623 delete
System logs will not be sent to 2001:9:6:40::623 anymore

(Cisco Controller) > show logging

Logging to buffer :
- Logging of system messages to buffer :
 - Logging filter level..... errors
 - Number of system messages logged..... 1316
 - Number of system messages dropped..... 6895
- Logging of debug messages to buffer ..... Disabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Cache of logging  ..... Disabled
- Cache of logging time(mins) ..... 10080
- Number of over cache time log dropped  ..... 0
Logging to console :
- Logging of system messages to console :
 - Logging filter level..... disabled
 - Number of system messages logged..... 0
 - Number of system messages dropped..... 8211
```

```
- Logging of debug messages to console .......... Enabled
 - Number of debug messages logged............... 0
 - Number of debug messages dropped.............. 0
Logging to syslog :
- Syslog facility................................ local0
- Logging of system messages to syslog :
 - Logging filter level.......................... errors
 - Number of system messages logged.............. 1316
 - Number of system messages dropped............. 6895
- Logging of debug messages to syslog ........... Disabled
 - Number of debug messages logged............... 0
 - Number of debug messages dropped.............. 0
- Number of remote syslog hosts.................. 0
- syslog over tls................................ Disabled
  - Host 0.......................................
  - Host 1.......................................
  - Host 2.......................................
Logging of RFC 5424............................. Disabled
Logging of Debug messages to file :
- Logging of Debug messages to file.............. Disabled
- Number of debug messages logged................ 0
- Number of debug messages dropped............... 0
Logging of traceback............................ Enabled
- Traceback logging level....................... errors
Logging of source file informational............ Enabled
Timestamping of messages.......................
- Timestamping of system messages................ Enabled
 - Timestamp format.............................. Date and Time
```

config logging syslog facility

リモート ホストへの発信 syslog メッセージのファシリティを設定するには、**config logging syslog facility** コマンドを使用します。

config logging syslog facility *facility_code*

構文の説明 *facility_code*

ファシリティ コード。次のいずれかを選択します。

- authorization：認証システム。ファシリティ レベル：4。
- auth-private：認証システム（プライベート）。ファシリティ レベル：10。
- cron：ファシリティあたりの Cron。ファシリティ レベル：9。
- daemon：システム デーモン。ファシリティ レベル：3。
- ftp：FTP デーモン。ファシリティ レベル：11。
- kern：カーネル。ファシリティ レベル：0。
- local0：ローカル用。ファシリティ レベル：16。
- local1：ローカル用。ファシリティ レベル：17。
- local2：ローカル用。ファシリティ レベル：18。
- local3：ローカル用。ファシリティ レベル：19。
- local4：ローカル用。ファシリティ レベル：20。
- local5：ローカル用。ファシリティ レベル：21。
- local6：ローカル用。ファシリティ レベル：22。
- local7：ローカル用。ファシリティ レベル：23。
- lpr：ラインプリンタ システム。ファシリティ レベル：6。
- mail：メール システム。ファシリティ レベル：2。
- news：USENET ニュース。ファシリティ レベル：7。

- sys12：システム用。ファシリティ レベル：12。
- sys13：システム用。ファシリティ レベル：13。
- sys14：システム用。ファシリティ レベル：14。
- sys15：システム用。ファシリティ レベル：15。
- syslog：syslog 自体。ファシリティ レベル：5。
- user：ユーザ プロセス。ファシリティ レベル：1。
- uucp：Unix-to-Unix コピー システム。ファシリティ レベル：8。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、発信 syslog メッセージのファシリティを認証に設定する例を示します。

```
(Cisco Controller) > config logging syslog facility authorization
```

関連コマンド

config logging syslog host

config logging syslog level

show logging

config logging syslog facility client

syslog ファシリティを AP に設定するには、**config logging syslog facility client** { **assocfail Dot11** | **associate Dot11** | **authentication** | **authfail Dot11** | **deauthenticate Dot11** | **disassociate Dot11** | **exclude**}{ **enable** | **disable**} コマンドを使用します。

config logging syslog facility *Client*

構文の説明

クライアント	ファシリティ クライアント。次の機能があります。 • assocfail Dot11：クライアントの関連付け失敗 syslog • associate Dot11：クライアントの関連付け syslog • authentication：クライアントの認証成功 syslog • authfail Dot11：クライアントの認証失敗 syslog • deauthenticate Dot11：クライアントの認証解除 syslog • disassociate Dot11：クライアントの関連付け解除 syslog • excluded：クライアントの除外 syslog

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドは、リリース 7.5 以前のリリースで導入されました。

次に、クライアントのファシリティ syslog ファシリティを設定する例を示します。

```
cisco controller config logging syslog facility client
```

関連コマンド

show logging flags client

config logging syslog facility ap

syslog ファシリティを AP に設定するには、 **config logging syslog facility ap**{ **associate** | **disassociate**}{ **enable** | **disable**} コマンドを使用します。

config logging syslog facility *AP*

構文の説明

AP	ファシリティ AP。次の機能があります。 • associate：AP の関連付け syslog • disassociate：AP の関連付け解除 syslog

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドは、リリース 7.5 以前のリリースで導入されました。

次に、AP の syslog ファシリティを設定する例を示します。

```
cisco controller config logging syslog facility ap
```

関連コマンド

show logging flags ap

config logging syslog level

リモート ホストへの syslog メッセージをフィルタするための重大度を設定するには、**config logging syslog level** コマンドを使用します。

config logging syslog level *severity_level*

構文の説明

severity_level	重大度。次のいずれかを選択します。 • 緊急：重大度 0 • アラート：重大度 1 • 重要：重大度 2 • エラー：重大度 3 • 警告：重大度 4 • 通知：重大度 5 • 情報：重大度 6 • デバッグ：重大度 7

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、syslog メッセージの重大度を 3 に設定する例を示します。

```
(Cisco Controller) > config logging syslog level 3
```

関連コマンド

config logging syslog host

config logging syslog facility

show logging

config loginsession close

アクティブなすべての Telnet セッションを閉じるには、**config loginsession close** コマンドを使用します。

config loginsession close {*session_id* | **all**}

構文の説明

session_id	閉じるセッションの ID。
all	すべての Telnet セッションを閉じます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクティブなすべての Telnet セッションを閉じる例を示します。

```
(Cisco Controller) > config loginsession close all
```

関連コマンド

show loginsession

config macfilter

Cisco ワイヤレス LAN コントローラで MAC フィルタ エントリを作成または削除するには、**config macfilter** {*add* | *delete*} コマンドを使用します。

config macfilter {**add** *client_MAC wlan_id* [*interface_name*] [*description*] [*macfilter_IP*] | **delete** *client_MAC*}

構文の説明

add	コントローラで MAC フィルタ エントリを追加します。
delete	コントローラで MAC フィルタ エントリを削除します。
MAC_addr	Client MAC address.
wlan_id	MAC フィルタ エントリをアソシエートする無線 LAN 識別子。値が 0 の場合、エントリをすべての無線 LAN にアソシエートします。
interface_name	（任意）インターフェイスの名前。インターフェイスを指定しない場合は **0** を入力してください。
description	（任意）二重引用符で囲まれた最大 32 文字の、インターフェイスの短い説明。 （注） *macfilterIP* を指定する場合、説明は必須です。
IP Address	（任意）ローカル MAC フィルタ データベースの IPv4 アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Cisco ワイヤレス LAN コントローラでクライアントを無線 LAN にローカルに追加するには、**config macfilter add** コマンドを使用します。このフィルタは RADIUS 認証プロセスをバイパスします。

リリース 7.6 と同様に、オプションの *macfilter_IP* は IPv4 アドレスだけをサポートしています。

次に、ワイヤレス LAN ID 1、インターフェイス名 labconnect、およびコントローラの MAC フィルタ IP 10.92.125.51 で MAC フィルタ エントリ 00:E0:77:31:A3:55 を追加する例を示します。

```
(Cisco Controller) > config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect"
10.92.125.51
```

関連コマンド

show macfilter

config macfilter ip-address

config macfilter description

MAC フィルタに説明を追加するには、**config macfilter description** コマンドを使用します。

config macfilter description *MAC addrdescription*

構文の説明

MAC addr	クライアント MAC アドレス
description	（任意）二重引用符で囲まれた説明（最大 32 文字）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC フィルタ 01 という説明を MAC アドレス 11:11:11:11:11:11 に設定する例を示します。

```
(Cisco Controller) > config macfilter description 11:11:11:11:11:11 "MAC Filter 01"
```

関連コマンド

show macfilter

config macfilter interface

MAC フィルタのクライアント インターフェイスを作成するには、**config macfilter interface** コマンドを使用します。

config macfilter interface *MAC_addr interface*

構文の説明

MAC addr	クライアント MAC アドレス
interface	インターフェイス名。値 0 は、名前なしに相当します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアント 11:11:11:11:11:11 で MAC フィルタ インターフェイス Lab01 を設定する例を示します。

```
(Cisco Controller) > config macfilter interface 11:11:11:11:11:11 Lab01
```

関連コマンド

show macfilter

config macfilter ip-address

パッシブ クライアントの IP アドレスを入力するには、**config macfilter ip-address** コマンドを使用します。

config macfilterip-address *MAC_addr IP Address*

構文の説明

MAC_addr	クライアントの MAC アドレス。
IP Address	パッシブ クライアントの IP アドレスを追加します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは IPv4 だけをサポートしています。

次に、パッシブ クライアントの IP アドレスを追加する例を示します。

```
(Cisco Controller) > config macfilter ip-address aa-bb-cc-dd-ee-ff 10.92.125.51
```

関連コマンド

show macfilter

config macfilter mac-delimiter

RADIUS サーバに送信される MAC アドレス の MAC デリミタ（コロン、ハイフン、なし、単一ハイフン）を設定するには、**config macfilter mac-delimiter** コマンドを使用します。

config macfilter mac-delimiter {**none** | **colon** | **hyphen** | **single-hyphen**}

構文の説明

none	デリミタを無効にします（xxxxxxxxxx など）。
colon	デリミタをコロンに設定します（xx:xx:xx:xx:xx:xx など）。
hyphen	デリミタをハイフンに設定します（xx-xx-xx-xx-xx-xx など）。
single-hyphen	デリミタを単一ハイフンに設定します（xxxxxx-xxxxxx など）。

コマンド デフォルト

デフォルトのデリミタは、ハイフンです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、aa:bb:cc:dd:ee:ff 形式で MAC アドレスを RADIUS サーバに送信するようにオペレーティング システムを設定する例を示します。

```
(Cisco Controller) > config macfilter mac-delimiter colon
```

次に、aa-bb-cc-dd-ee-ff 形式で MAC アドレスを RADIUS サーバに送信するようにオペレーティング システムを設定する例を示します。

```
(Cisco Controller) > config macfilter mac-delimiter hyphen
```

次に、aabbccddeeff 形式で MAC アドレスを RADIUS サーバに送信するようにオペレーティング システムを設定する例を示します。

```
(Cisco Controller) > config macfilter mac-delimiter none
```

関連コマンド

show macfilter

config macfilter radius-compat

Cisco ワイヤレス LAN コントローラと選択した RADIUS サーバとの互換性を設定するには、**config macfilter radius-compat** コマンドを使用します。

config macfilter radius-compat {**cisco** | **free** | **other**}

構文の説明

cisco	Cisco ACS 互換性モード（パスワードはサーバの MAC アドレス）を設定します。
free	Free RADIUS サーバ互換性モード（パスワードは非公開）を設定します。
other	他のサーバ動作（パスワードは不要）を設定します。

コマンド デフォルト

other

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは IPv4 だけをサポートしています。

次に、Cisco ACS 互換性モードを「その他」に設定する例を示します。

```
(Cisco Controller) > config macfilter radius-compat other
```

関連コマンド

show macfilter

config macfilter wlan-id

MAC フィルタの無線 LAN ID を変更するには、**config macfilter wlan-id** コマンドを使用します。

config macfilter wlan-id *MAC_addr WLAN_id*

構文の説明

MAC addr	クライアント MAC アドレス
WLAN_id	アソシエートする無線 LAN 識別子。値 0 は使用できません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC フィルタ 11:11:11:11:11:11 のクライアントの無線 LAN ID 2 を変更する例を示します。

```
(Cisco Controller) > config macfilter wlan-id 11:11:11:11:11:11 2
```

関連コマンド

show macfilter

show wlan

config mdns ap

アクセス ポイントでマルチキャスト ドメイン ネーム システム（mDNS）スヌーピングを設定するには、**config mdns ap** コマンドを使用します。

config mdns ap {**enable** {*ap_name* | **all**} [**vlan** *vlan_id*] | **disable** {*ap_name* | **all**} | **vlan** {**add** | **delete**} *vlan ap_name*}

構文の説明

enable	アクセス ポイントで mDNS スヌーピングを有効にします。
ap_name	mDNS スヌーピングを設定する必要があるアクセス ポイントの名前。
all	すべてのアクセス ポイントで mDNS スヌーピングを設定します。
vlan	（任意）アクセス ポイントが mDNS パケットをスヌープして転送する VLAN を設定します。
vlan_id	VLAN 識別番号。
disable	アクセス ポイントで mDNS スヌーピングを無効にします。
add	アクセス ポイントが mDNS パケットをスヌープして Cisco ワイヤレス LAN コントローラ（WLC）に転送する VLAN を追加します。mDNS アクセス ポイントには最大 10 の VLAN を設定できます。
delete	アクセス ポイントが mDNS パケットをスヌープして Cisco WLC に転送する VLAN を削除します。

コマンド デフォルト

mDNS 対応アクセス ポイントは、デフォルトでアクセス VLAN またはネイティブ VLAN をスヌープします。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

アクセス ポイントで mDNS スヌーピングを有効にすると、アクセス ポイントは Cisco WLC に表示されない VLAN 上の有線サービスをスヌープできるようになります。mDNS スヌーピングはローカル モードおよびモニタ モードのアクセス ポイントでのみサポートされています。アクセス ポイントはアクセス モードまたはトランク モードになっている必要があります。アクセス ポイントがトランク モードの場合は、アクセス ポイントが mDNS パケットをスヌープして転送する Cisco WLC で VLAN を設定する必要があります。アクセス ポイントが mDNS ク

エリをスヌープして送信するには、Cisco WLC からネイティブ VLAN も設定する必要があります。また、アクセス ポイントは、ネイティブ VLAN でパケットにタグ付けします。

グローバル mDNS スヌーピングは、mDNS アクセス ポイント スヌーピングに優先されます。

次に、アクセス ポイントで mDNS スヌーピングを有効にし、アクセス ポイントが mDNS パケットをスヌープする必要がある VLAN を設定する例を示します。

```
(Cisco Controller) > config mdns ap enable vlan 1
```

config mdns profile

マルチキャストDNS（mDNS）プロファイルを設定して、プロファイルにサービスを関連付けるには、**config mdns profile** コマンドを使用します。

config mdns profile {**create** | **delete** | **service** {**add** | **delete**} *service _name profile_name*

構文の説明

create	mDNS プロファイルを作成します。
delete	mDNS プロファイルを削除します。プロファイルがインターフェイス グループ、インターフェイス、または WLAN に関連付けられている場合は、エラーが表示されます。
service	mDNS サービスを設定します。
add	mDNS プロファイルに mDNS サービスを追加します。
delete	mDNS プロファイルから mDNS サービスを削除します。
service -name	mDNS サービスの名前。
profile_name	mDNS プロファイルの名前。最大 16 個のプロファイルを作成できます。

コマンド デフォルト

デフォルトでは、コントローラに mDNS プロファイル、デフォルト mdns プロファイルがあります。このデフォルト プロファイルは削除できません。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

使用上のガイドライン

新しいプロファイルを作成した後、インターフェイス グループ、インターフェイス、またはWLANにプロファイルをマッピングする必要があります。クライアントはプロファイルに関連付けられたサービスのみのサービス アドバタイズメントを受信します。コントローラはインターフェイス グループに関連付けられたプロファイルに最高の優先順位を与えます。次にインターフェイス プロファイル、WLAN プロファイルが続きます。各クライアントは、優先順位に従ってプロファイルにマップされます。

デフォルトでは、コントローラに mDNS プロファイル、デフォルト mdns プロファイルがあります。このデフォルト プロファイルは削除できません。

次に、mDNS profile1 に Apple TV の mDNS サービスを追加する例を示します。

```
(Cisco Controller) > config mdns profile create profile1 Apple TV
```

関連コマンド

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config mdns query interval

マルチキャスト DNS（mDNS）サービスのクエリ間隔を設定するには、**config mdns query interval** コマンドを使用します。

config mdns query interval *interval_value*

構文の説明

interval_value	設定可能な分単位の mDNS クエリ間隔。クエリ間隔とは、コントローラがマスター サービス データベースで定義されているすべてのサービスに定期的にクエリを送信する頻度です。範囲は 10 ～ 120 です。

コマンド デフォルト

mDNS サービスのデフォルトのクエリ間隔は 15 分です。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

使用上のガイドライン

コントローラは、マスター サービス データベースで mDNS サービスが利用できる場合にのみ、このサービスのアドバタイズメントをスヌーピングおよび学習します。mDNS は宛先アドレスとしてマルチキャスト IP アドレス 224.0.0.251 を使用し、UDP 宛先ポートとして 5353 を使用します。

次に、mDNS サービスのクエリ間隔を 20 分間に設定する例を示します。

```
(Cisco Controller) > config mdns query interval 20
```

関連コマンド

config mdns profile

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config mdns service

マスター サービス データベースにマルチキャスト DNS（mDNS）サービスを設定するには、**config mdns service** コマンドを使用します。

次のコマンドは、リリース 7.5 以降のリリースで使用できます。

config mdns service {**create** *service_name service_string* **origin** {**Wireless** | **Wired** | **All**} **lss** {**enable** | **disable**} [**query** {**enable** | **disable**}] | **lss** {**enable** | **disable**} {*service_name* | **all**} | **priority-mac** {**add** | **delete**} *priority-mac service_name* [**ap-group** *ap-group-name*] | **origin** {**Wireless** | **Wired** | **All**} {*service_name* | **all**}}

構文の説明

create	マスターサービスデータベースに新しいmDNSサービスを追加します。
service_name	mDNS サービスの名前。たとえば、Air Tunes、iTunes Music Sharing、FTP、Apple File Sharing Protocol（AFP）などです。
service_string	mDNS サービスに関連付けられた一意の文字列。たとえば、_airplay._tcp.local. は、AppleTV に関連付けられたサービス文字列です。
delete	マスターサービスデータベースからmDNSサービスを削除します。サービスを削除する前に、コントローラはプロファイルがサービスを使用しているかどうかを確認します。 （注） サービスを削除する前に、すべてのプロファイルからサービスを削除する必要があります。
query	mDNS サービスのクエリー ステータスを設定します。
enable	コントローラによる mDNS サービスの定期クエリーをイネーブルにします。
disable	コントローラによる mDNS サービスの定期クエリーをディセーブルにします。
origin	mDNS サービスの発信元を設定します。サービスの発信元を有線またはワイヤレスに制限できます。
Wireless	mDNS サービスの発信元をワイヤレスとして設定します。
Wired	mDNS サービスの発信元を有線として設定します。
All	mDNS サービスの発信元をワイヤレスまたは有線として設定します。

lss	1 つのサービスまたはすべての mDNS サービスのロケーション固有サービス（LSS）を設定します。LSS は登録済みのサービスプロバイダーには適用されません。クエリ元クライアントがユーザと一致する場合は、登録済みのサービス プロバイダーが常に含まれます。有線のみに設定されたサービスについては LSS を設定できません。
all	すべての mDNS サービスの LSS を設定します。
priority-mac	サービスプロバイダーデバイスのMACアドレスを設定します。このデバイスは、サービス プロバイダー データベースがいっぱいであっても優先されます。
add	優先されるサービス プロバイダー デバイスの MAC アドレスを追加します。 1 つのサービスについて最大 50 の MAC アドレスを設定できます。
delete	優先リストからサービス プロバイダー デバイスの MAC アドレスを削除します。
priority-mac	優先する必要があるサービス プロバイダー デバイスの MAC アドレス。MACアドレスはサービスごとに一意である必要があります。
ap-group	有線サービスプロバイダーのアクセスポイントグループを設定します。これらのサービスプロバイダーは他のサービス プロバイダーよりも優先されます。クライアントの mDNS クエリがこの AP グループから発信されると、優先 MAC アドレスを持つ有線エントリとアクセス ポイント グループのリストが集約応答の最初に示されます。
ap-group-name	サービスプロバイダーが属するアクセスポイントグループの名前。

コマンド デフォルト

デフォルトでは、LSS は無効になっていますが、検出されるすべてのサービスに関して有効になります。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。
7.5	このコマンドが変更されました。**origin**、**Wireless**、**Wired**、**All**、**lss**、**priority-mac**、**add**、**delete**、**ap-group** キーワードと *priority-mac ap-group-name* 引数が追加されました。

使用上のガイドライン

リリース7.5以降のリリースでは、各コントローラモデルのサービスプロバイダーの最大数は次のとおりです。

- Cisco 5500 シリーズ コントローラと Cisco 2500 シリーズ コントローラ：6400
- Cisco ワイヤレス サービス モジュール 2：6400
- Cisco 8500 シリーズ コントローラと Cisco 7500 シリーズ コントローラ：16000

サービスのLSSが有効になっている場合、発信元がワイヤレスに設定されているサービスを有線に変更できません。

次に、HTTP mDNS サービスをマスター サービス データベースに追加して、発信元をワイヤレスに設定し、そのサービスの LSS を有効にする例を示します。

```
(Cisco Controller) > config mdns service create http _http._tcp.local. origin wireless
lss enable
```

次に、HTTP サービス プロバイダー デバイスの優先 MAC アドレスを追加する例を示します。

```
(Cisco Controller) >config mdns service priority-mac add 44:03:a7:a3:04:45 http
```

config mdns snooping

Cisco WLC でグローバル マルチキャスト DNS（mDNS）スヌーピングを有効または無効にするには、**config mdns snooping** コマンドを使用します。

config mdns snooping {**enable** | **disable**}

構文の説明

enable	Cisco WLC でグローバル mDNS スヌーピングを有効にします。
disable	Cisco WLC でグローバル mDNS スヌーピングを無効にします。

コマンド デフォルト

デフォルトでは、Cisco WLC で mDNS スヌーピングが有効になっています。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

使用上のガイドライン

mDNS サービス検出では、ローカル ネットワーク上のサービスをアナウンスし、検出するための手段を提供します。mDNS は、IP マルチキャストで DNS クエリを実行します。mDNS はゼロ コンフィギュレーション IP ネットワーキングをサポートします。

次に、IGMP スヌーピングを有効にする例を示します。

```
(Cisco Controller) > config mdns snooping enable
```

関連コマンド

config mdns query interval

config mdns service

config mdns profile

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config mdns policy enable

mDNS ポリシーを設定するには、**config mdns policy enable | disable** コマンドを使用します。

config mdnspolicyenable | disable

構文の説明

policy	mDNS ポリシーの名前。
enable	コントローラによる mDNS サービスのポリシーを有効にします。
disable	コントローラによる mDNS サービスのポリシーを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドは 8.0 リリース以降で使用できます。

例

次に、mDNS ポリシーを設定する例を示します。

```
(Cisco Controller) >config mdns
  policy enable
```

config mdns policy service-group

mDNS ポリシー サービス グループを作成または削除するには、**config mdns policy service-group** コマンドを使用します。

config mdns policy service-group {**create** | **delete**} *service-group-name*

構文の説明

create	mDNS サービス グループを作成します。
delete	mDNS サービス グループを削除します。
service-group-name	サービス グループの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

例

次に、mDNS サービス グループを削除する例を示します。

```
(Cisco Controller) >config mdns policy service-group create <service-group-name>
```

config mdns policy service-group parameters

サービス グループのパラメータを設定するには、 **config mdns policy service-group** コマンドを使用します。

config mdnspolicyservice-group device-mac add *service-group-name mac-addr device name* **location-type** *[AP_LOCATION | AP_NAME |AP_GROUP]* **device-location** *[location string |any | same]*

構文の説明

device-mac	サービス プロバイダー デバイスの MAC アドレスを設定します。
add	サービスプロバイダーデバイスのサービス グループ名を追加します。
service-group-name	mDNS サービス グループの名前。
device-name	サービス プロバイダーが属しているデバイスの名前。
location type	サービスプロバイダーデバイスのロケーション タイプを設定します。
[AP_LOCATION | AP_NAME | AP_GROUP]	アクセス ポイントの名前、位置、グループ。
device-location	サービス プロバイダーが属しているデバイスの位置を設定します。
[location string |any | same]	デバイスの位置を表す文字列。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

例

次に、サービス プロバイダー デバイスのロケーション タイプを設定する例を示します。

```
(Cisco Controller) >config mdns policy service-group location type [AP_LOCATION | AP_NAME
 | AP_GROUP]
```

config mdns policy service-group user-name

mDNS サービス グループのユーザ ロールを設定するには、**config mdns policy service-group user-name add | delete <service-group-name> <user-role-name>** コマンドを使用します。

config mdnspolicyservice-groupuser-nameadd | delete*service-group-name user-name*

構文の説明

user-name	mDNS サービス グループのユーザの名前を設定します。
service-group-name	mDNS サービス グループの名前。
user-name	mDNS サービス グループのユーザ ロールの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

例

次に、mDNS サービス グループのユーザ名を追加する例を示します。

```
(Cisco Controller) >config mdns policy service-group user-name add <service-group-name>
 <user-role-name>
```

config mdns policy service-group user-role

mDNS サービス グループのユーザ ロールを設定するには、**config mdns policy service-group user-role add | delete <service-group-name> <user-role-name>** コマンドを使用します。

config mdnspolicyservice-groupuser-roleadd | delete*service-group-name user-role-name*

構文の説明

user-role	mDNS サービス グループのユーザ ロールを設定します。
service-group-name	mDNS サービス グループの名前。
user-role-name	mDNS サービス グループのユーザ ロールの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

例

次に、mDNS サービス グループのユーザ ロール詳細情報を追加する例を示します。

```
(Cisco Controller) >config mdns policy service-group user-role add <service-group-name>
 <user-role-name>
```

config media-stream multicast-direct

メディア ストリーム マルチキャスト ダイレクトを設定するには、**config media-stream multicast direct** コマンドを使用します。

config media-stream multicast-direct {**enable** | **disable**}

構文の説明

enable	メディア ストリームを有効にします。
disable	メディア ストリームを無効にします。

コマンド デフォルト

なし。

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。

次に、メディア ストリーム マルチキャスト ダイレクト設定を有効にする例を示します。

```
> config media-stream multicast-direct enable
```

次に、メディア ストリーム マルチキャスト ダイレクト設定を無効にする例を示します。

```
> config media-stream multicast-direct disable
```

関連コマンド

config 802.11 media-stream video-redirect

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream message

メッセージ設定のさまざまなパラメータを設定するには、**config media-stream message** コマンドを使用します。

config media-stream message {**state** [**enable** | **disable**] | **url** *url* | **email** *email* | **phone** *phone_number* | **note** *note*}

構文の説明

state	メディア ストリーム メッセージの状態を指定します。
enable	（任意）セッション アナウンス メッセージの状態を有効にします。
disable	（任意）セッション アナウンス メッセージの状態を無効にします。
url	URL を設定します。
url	セッション アナウンス URL。
email	電子メール ID を設定します。
email	セッション アナウンスの電子メールを指定します。
phone	電話番号を設定します。
phone_number	セッション アナウンスの電話番号。
note	メモを設定します。
note	セッション アナウンスのメモ。

コマンド デフォルト

ディセーブル

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。

次に、セッション アナウンスメント メッセージの状態を有効にする例を示します。

```
> config media-stream message state enable
```

次に、セッション アナウンスの電子メール アドレスを設定する例を示します。

```
> config media-stream message mail abc@co.com
```

関連コマンド

config media-stream

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream add

さまざまなグローバル メディア ストリーム設定を行うには、**config media-stream add** コマンドを使用します。

config media-stream add multicast-direct *media_stream_name start-IP end-IP* [**template** {**very coarse** | **coarse** | **ordinary** | **low-resolution** | **med-resolution** | **high-resolution**} | **detail** {*bandwidth packet-size* {**periodic** | **initial**}} **qos** *priority* {**drop** | **fallback**}

構文の説明

multicast-direct	マルチキャスト ダイレクト設定のメディア ストリームを指定します。
media_stream_name	メディア ストリームの名前。
start-IP	IP マルチキャストの宛先開始アドレス。
end-IP	IP マルチキャストの宛先終了アドレス。
template	（任意）テンプレートからのメディアストリームを設定します。
very coarse	非常に粗いテンプレートを適用します。
coarse	粗いテンプレートを適用します。
ordinary	通常のテンプレートを適用します。
low-resolution	低解像度のテンプレートを適用します。
med-resolution	通常の解像度のテンプレートを適用します。
high-resolution	高解像度のテンプレートを適用します。
detail	特定のパラメータでメディア ストリームを設定します。
bandwidth	予想される最大ストリーム帯域幅。
packet-size	平均パケット サイズ。
periodic	定期的なアドミッション評価を指定します。
initial	最初のアドミッション評価を指定します。
qos	AIR QoS クラス（ビデオのみ）。
priority	メディア ストリームの優先順位。
drop	ストリームが定期的な再評価でドロップされるように指定します。

fallback	定期的な再評価でストリームがベストエフォートクラスに降格されるかどうかを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。

次に、新しいメディア ストリームを設定する例を示します。

```
> config media-stream add multicast-direct abc 227.8.8.8 227.9.9.9 detail 2 150 periodic
 video 1 drop
```

関連コマンド

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream admit

メディア ストリーム グループのトラフィックを許可するには、**config media-stream admit** コマンドを使用します。

config media-stream admit *media_stream_name*

構文の説明

media_stream_name	メディア ストリームのグループ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

メディア ストリーム グループのトラフィックを許可しようとすると、IGMP スヌーピングを無効にして再度有効にすることを求めるプロンプトが表示されます。また、マルチキャスト トラフィックの異常がすべてのクライアントに対して発生する場合があります。

次に、メディア ストリーム グループのトラフィックを許可する例を示します。

```
(Cisco Controller) > config media-stream admit MymediaStream
```

関連コマンド

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream deny

メディア ストリーム グループのトラフィックをブロックするには、**config media-stream deny** コマンドを使用します。

構文の説明

media_stream_name	メディア ストリームのグループ名。

config media-stream deny *media_stream_name*

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

メディアストリーム グループのトラフィックをブロックしようとすると、IGMP スヌーピングを無効にして再度有効にすることを求めるプロンプトが表示されます。また、マルチキャスト トラフィックの異常がすべてのクライアントに対して発生する場合があります。

次に、メディア ストリーム グループのトラフィックをブロックする例を示します。

```
(Cisco Controller) > config media-stream deny MymediaStream
```

関連コマンド

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream delete

さまざまなグローバル メディア ストリーム設定を行うには、**config media-stream delete** コマンドを使用します。

config media-stream delete *media_stream_name*

構文の説明

media_stream_name	メディア ストリームの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。

次に、abc という名前のメディア ストリームを削除する例を示します。

```
(Cisco Controller) > config media-stream delete abc
```

関連コマンド

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config memory monitor errors

メモリ エラーおよびメモリ リークのモニタリングを有効または無効にするには、**config memory monitor errors** コマンドを使用します。

config memory monitor errors {**enable** | **disable**}

⚠

注意 **config memory monitor** コマンドはシステムに悪影響を及ぼす可能性があるので、Cisco TAC の指示を受けた場合に限り実行する必要があります。

構文の説明

enable	メモリ設定のモニタリングをイネーブルにします。
disable	メモリ設定のモニタリングをディセーブルにします。

コマンド デフォルト

メモリ エラーおよびリークのモニタリングは、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

操作について知識があり、問題が検出され、トラブルシューティング情報の収集が行われている場合を除き、**config memory monitor** コマンドのデフォルトの変更は慎重に行うようにしてください。

次に、コントローラのメモリ エラーおよびリークのモニタリングを有効にする例を示します。

```
(Cisco Controller) > config memory monitor errors enable
```

関連コマンド

config memory monitor leaks

debug memory

show memory monitor

config memory monitor leaks

2 つのメモリしきい値の間で自動リーク分析を実行するようにコントローラを設定するには、**config memory monitor leaks** コマンドを使用します。

config memory monitor leaks *low_thresh high_thresh*

注意 **config memory monitor** コマンドはシステムに悪影響を及ぼす可能性があるので、Cisco TAC の指示を受けた場合に限り実行する必要があります。

構文の説明

low_thresh	空きメモリがクラッシュする下限値。この値は 10,000 KB 未満に設定できません。
high_thresh	コントローラが auto-leak-analysis モードになる下限値。「使用上のガイドライン」の項を参照してください。

コマンド デフォルト

low_thresh のデフォルト値は 10000 KB であり、*high_thresh* のデフォルト値は 30000 KB です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

（注） 操作について知識があり、問題が検出され、トラブルシューティング情報の収集が行われている場合を除き、**config memory monitor** コマンドのデフォルトの変更は慎重に行うようにしてください。

メモリ リークのおそれがある場合は、このコマンドを使用します。

空きメモリが *low_thresh* しきい値を下回ると、システムがクラッシュしてクラッシュ ファイルが生成されます。このパラメータのデフォルト値は 10,000 KB です。この値より低い値に設定できません。

high_thresh しきい値は、現在の空きメモリの大きさ以上に設定してください。このようにすると、システムは自動リーク分析モードになります。空きメモリの大きさが、指定された *high_thresh* しきい値を下回ると、メモリ割り当てのトラッキングと解放のプロセスが開始します。その結果、**debug memory events enable** コマンドによってすべての割り当てと空きメモリが表示され、 **show memory monitor detail** コマンドによってメモリ リークの疑いの検出が開始されます。

次に、auto-leak-analysis モードのしきい値を、下限しきい値 12000 KB と上限しきい値 35000 KB に設定する例を示します。

```
(Cisco Controller) > config memory monitor leaks 12000 35000
```

関連コマンド

config memory monitor leaks

debug memory

show memory monitor

config mesh alarm

屋外メッシュ アクセス ポイントのアラーム設定を行うには、**config mesh alarm** コマンドを使用します。

config mesh alarm {**max-hop** | **max-children** | **low-snr** | **high-snr** | **association** | **parent-change count**} *value*

構文の説明

max-hop	メッシュ ネットワーク上のトラフィックでアラームをトリガーするまでの最大ホップ カウントを設定します。有効な値は 1 ～ 16 です。
max-children	メッシュルートアクセスポイント（RAP）に割り当てることのできるメッシュアクセスポイント（MAP）の最大数を設定します。この数を超えると、アラームがトリガーされます。有効な値は 1 ～ 16 です。
low-snr	信号対雑音比（SNR）の下限値を設定します。この値を下回ると、アラームがトリガーされます。有効な値は 1 ～ 30 です。
high-snr	SNR の上限値を設定します。この値を超えると、アラームがトリガーされます。有効な値は 1 ～ 30 です。
association	メッシュ アラームのアソシエーション数値を設定します。この値を超えると、アラームがトリガーされます。有効な値は 1 ～ 30 です。
parent-change count	MAP で RAP アソシエーションを変更できる回数を設定します。この回数を超えると、アラームがトリガーされます。有効な値は 1 ～ 30 です。
value	この値を上回る、または下回るとアラームが生成される、トリガー値。有効な値は、コマンドごとに異なります。

コマンド デフォルト

コマンドおよび引数の値の範囲については、「構文の説明」の項を参照してください。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、最大ホップのしきい値を 8 に設定する例を示します。

```
(Cisco Controller) >config mesh alarm max-hop 8
```

次に、SNR の上限しきい値を 25 に設定する例を示します。

```
(Cisco Controller) >config mesh alarm high-snr 25
```

config mesh astools

屋外メッシュ アクセス ポイントの孤立防止機能をグローバルに有効または無効にするには、**config mesh astools** コマンドを使用します。

config mesh astools {**enable** | **disable**}

構文の説明

enable	すべての屋外メッシュ アクセス ポイントに対してこの機能を有効にします。
disable	すべての屋外メッシュ アクセス ポイントに対してこの機能を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての屋外メッシュ アクセス ポイントの孤立防止機能を有効にする例を示します。

```
(Cisco Controller) >config mesh astools enable
```

config mesh backhaul rate-adapt

屋内および屋外メッシュ アクセス ポイントに対してバックホール送信レート適応（ユニバーサル アクセス）をグローバルに設定するには、**config mesh backhaul rate-adapt** コマンドを使用します。

config mesh backhaul rate-adapt ［**all** | **bronze** | **silver** | **gold** | **platinum**］｛**enable** | **disable**｝

構文の説明

all	（任意）メッシュ アクセス ポイントでユニバーサル アクセス権限を許可します。
bronze	（任意）メッシュ アクセス ポイントでバックグラウンド レベルのクライアント アクセス権限が許可されます。
silver	（任意）メッシュ アクセス ポイントでベストエフォート レベルのクライアント アクセス権限が許可されます。
gold	（任意）メッシュ アクセス ポイントでビデオ レベルのクライアント アクセス権限が許可されます。
platinum	（任意）メッシュ アクセス ポイントで音声レベルのクライアント アクセス権限が許可されます。
enable	メッシュ アクセス ポイントのこのバックホール アクセス レベルを有効にします。
disable	メッシュ アクセス ポイントのこのバックホール アクセス レベルを無効にします。

コマンド デフォルト

メッシュ アクセス ポイントのバックホール アクセス レベルは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用するには、クライアント アクセスを持つメッシュ バックホールを **config mesh client-access** コマンドを使用して有効にする必要があります。

（注） この機能をイネーブルにすると、すべてのメッシュ アクセス ポイントがリブートします。

次にバックホール クライアント アクセスをベストエフォート レベルに設定する例を示します。

```
(Cisco Controller) >config mesh backhaul rate-adapt silver
```

config mesh backhaul slot

ダウンリンクのバックホールとしてスロットの無線を設定するには、**config mesh backhaul slot** コマンドを使用します。

config mesh backhaul slot *slot_id* {**enable** | **disable**} *cisco_ap*

構文の説明

slot_id	0～2 の間のスロット番号。
enable	ダウンリンクのバックホールとして入力されたスロットの無線を有効にします。
disable	ダウンリンクのバックホールとして入力されたスロットの無線を無効にします。
cisco_ap	バックホールを有効にするか、無効にする必要があるセクターのルート AP の名前。

コマンド デフォルト

ダウンリンクのバックホールとして入力されたスロットの無線は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

2.4 GHz の場合、スロット 0 と 1 のみが有効です。スロット 0 が有効になっている場合、スロット 1 が自動的に無効になります。スロット 0 が無効になっている場合、スロット 1 が自動的に有効になります。

次に、ルート AP myrootap1 の優先バックホールとしてスロット 1 を有効にする例を示します。

```
(Cisco Controller) >config mesh backhaul slot 1 enable myrootap1
```

config mesh battery-state

Cisco Aironet 1520 シリーズのメッシュ アクセス ポイントのバッテリ状態を設定するには、**config mesh battery-state** コマンドを使用します。

config mesh battery-state {**enable** | **disable**} {**all** | *cisco_ap* }

構文の説明

enable	1520 シリーズのメッシュ アクセス ポイントのバッテリ状態を有効にします。
disable	1520 シリーズのメッシュ アクセス ポイントのバッテリ状態を無効にします。
all	すべてのメッシュ アクセス ポイントにこのコマンドを適用します。
cisco_ap	特定のメッシュ アクセス ポイント。

コマンド デフォルト

バッテリ状態は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次にバックホール クライアント アクセスをベストエフォート レベルに設定する例を示します。

```
(Cisco Controller) >config mesh battery-state enable all
```

config mesh client-access

屋内または屋外のメッシュ アクセス ポイントでメッシュ バックホールへのクライアント アクセスを有効または無効にするには、**config mesh client-access** コマンドを使用します。

config mesh client-access {**enable** [**extended**] | **disable**}

構文の説明

enable	メッシュ アクセス ポイントのバックホール 802.11a 無線経由での無線クライアント アソシエーションを許可します。
extended	（任意）バックホール アクセス ポイントに対する両方のバックホール無線上でクライアント アクセスを有効にします。
disable	802.11a 無線をバックホール トラフィックに制限し、802.11b/g 無線経由でのクライアント アソシエーションだけを許可します。

コマンド デフォルト

クライアント アクセスは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

バックホール インターフェイス（802.11a 無線）は、プライマリ イーサネット インターフェイスとして機能します。バックホールはネットワーク内のトランクとして機能し、無線ネットワークと有線ネットワークとの間のすべての VLAN トラフィックを伝送します。プライマリ イーサネット インターフェイスに必要な設定はありません。

この機能が有効の場合、メッシュ アクセス ポイントで、802.11a 無線上で無線クライアント アソシエーションを許可します。つまり、152x メッシュ アクセス ポイントは、同一の 802.11a 無線経由でバックホール トラフィックと 802.11a クライアント トラフィックの両方を伝送できます。

この機能を無効にすると、メッシュ アクセス ポイントでは、802.11a 無線でバックホール トラフィックが伝送され、クライアント アソシエーションは 802.11b/g 無線のみで行われます。

次に、802.11a 無線上で無線クライアント アソシエーションを許可するために拡張されたクライアント アクセスを有効にする例を示します。

```
(Cisco Controller) >config mesh client-access enable extended
Enabling client access on both backhaul slots
 Same BSSIDs will be used on both slots
 All Mesh AP will be rebooted
 Are you sure you want to start? (y/N)Y
```

次に、無線クライアントアソシエーションを 802.11b/g 無線に制限する例を示します。

```
(Cisco Controller) >config mesh client-access disable
All Mesh AP will be rebooted
Are you sure you want to start? (Y/N) Y
Backhaul with client access is canceled.
```

config mesh convergence

すべてのメッシュ アクセス ポイントでメッシュ コンバージェンス方式を設定するには、**config mesh convergence** コマンドを使用します。

config mesh convergence {**fast** [**standard**] | **very-fast**} *all*

構文の説明

fast	高速コンバージェンス方式を設定します。
standard	標準コンバージェンス方式を設定します。
very-fast	超高速コンバージェンス方式を設定します。
all	選択したメッシュ コンバージェンス方式をすべてのメッシュ アクセス ポイントで設定します。

コマンド デフォルト

デフォルトのメッシュ コンバージェンス方式は標準です。

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

標準コンバージェンス方式は、リリース 7.6 以降で使用できます。高速および超高速コンバージェンス方式は、リリース 8.0 以降で使用できます。

次の表は各種コンバージェンス方式を示します。

コンバージェンス方式	親損失のタイマー（秒単位）。	チャンネルごとの検索のタイマー（秒単位）。	親、ネイバー キープアライブのタイマー（秒単位）。
Standard	21	3	3
Fast	7	2	3
Very Fast	4	2	1.5

次に、メッシュ コンバージェンスを Standard に設定する例を示します。

```
(Cisco Controller) >config mesh convergence standard all
```

config mesh ethernet-bridging allow-bpdu

有線メッシュ アップリンクへの STP BPDU を設定するには、**config mesh ethernet-bridging allow-bpdu** コマンドを使用します。

config mesh ethernet-bridging allow-bpdu {**enable** | **disable**}

構文の説明

enable	有線メッシュ アップリンクへの STP BPDU を有効にします。
disable	有線メッシュ アップリンクへの STP BPDU を無効にします。

コマンド デフォルト

無効

コマンド履歴

リリース	変更内容
8.0.110.0	このコマンドが導入されました。

使用上のガイドライン

VLAN 透過性が有効になっている場合、Cisco WLC ではこのコマンドを使用できません。

config mesh ethernet-bridging vlan-transparent

メッシュ アクセス ポイントでイーサネット ブリッジド トラフィックの VLAN タグを処理する方法を設定するには、**config mesh ethernet-bridging vlan-transparent** コマンドを使用します。

config mesh ethernet-bridging vlan-transparent {**enable** | **disable**}

構文の説明

enable	パケットをタグなしであるかのようにブリッジします。
disable	すべてのタグ付きパケットをドロップします。

コマンド デフォルト

パケットをタグなしであるかのようにブリッジします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、イーサネット パケットをタグなしとして設定する例を示します。

```
(Cisco Controller) >config mesh ethernet-bridging vlan-transparent enable
```

次に、タグ付きイーサネット パケットをドロップする例を示します。

```
(Cisco Controller) >config mesh ethernet-bridging vlan-transparent disable
```

config mesh full-sector-dfs

メッシュ アクセス ポイントでフルセクタの動的周波数選択（DFS）をグローバルに有効または無効にするには、**config mesh full-sector-dfs** コマンドを使用します。

config mesh full-sector-dfs {**enable** | **disable**}

構文の説明

enable	メッシュ アクセス ポイントの DFS を有効にします。
disable	メッシュ アクセス ポイントの DFS を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、レーダー信号の検出時にチャネル変更の調整を行うようにメッシュ セクターに指示します。たとえば、メッシュ アクセス ポイント（MAP）がレーダー信号を検出すると、MAP はルート アクセス ポイント（RAP）に通知し、RAP はセクター変更を開始します。

このセクターに属するすべての MAP および RAP は新しいチャネルに移動します。これにより、現在のバックホール チャネルでレーダーが検出され、バックアップとして使用可能な他の有効な親が存在しない場合に、MAP が孤立する可能性を低減します。

各セクターの変更により、（DFS 標準で定められているように）ネットワークが 60 秒間応答を停止します。

30 分後には、RAP は以前に設定されたチャネルに戻ります。これは、RAP のチャネルでレーダーが頻繁に検出される場合、この RAP に別のチャネルを設定し、コントローラでレーダーの影響を受けたチャネルを除外することが重要であることを意味します。

次に、メッシュ アクセス ポイントでフルセクタの DFS を有効にする例を示します。

```
(Cisco Controller) >config mesh full-sector-dfs enable
```

config mesh linkdata

アクセス ポイントの外部 MAC フィルタリングを有効にするには、**config mesh linkdata** コマンドを使用します。

config mesh linkdata *destination_ap_name*

構文の説明

destination_ap_name	MACアドレス フィルタリングの宛先アクセス ポイント名。

コマンド デフォルト

外部 MAC フィルタリングは無効になっています。

使用上のガイドライン

（注） **config mesh linktest** コマンドと **config mesh linkdata** コマンドは、同時に使用して、発信元アクセス ポイントと宛先アクセス ポイントで情報を照合するように設計されています。この情報を取得するには、まず *dest_ap* 引数でデータのリンク元になるアクセス ポイントを指定して **config mesh linktest** コマンドを実行します。このコマンドが完了して、同じ宛先アクセス ポイントをリスト表示する **config mesh linkdata** コマンドを実行すると、リンク データが表示されます（例を参照）。

デフォルトでは、MAC フィルタリングは、コントローラ上のローカル MAC フィルタを使用します。

外部 MAC フィルタ認証が有効であり、MAC アドレスがローカル MAC フィルタで検出されない場合には、外部 RADIUS サーバの MAC アドレスが使用されます。

MAC フィルタリングにより、外部サーバで定義されていないアクセスポイントの参加を防止して、不正なメッシュ アクセス ポイントからネットワークを保護します。

メッシュ ネットワーク内で外部認証を利用するには、次の設定が必要です。

- AAA サーバとして使用する RADUIS サーバをコントローラで設定する必要があります。
- コントローラも、RADIUS サーバで設定する必要があります。
- 外部認証および認証用に設定されたメッシュ アクセス ポイントは、RADIUS サーバのユーザ リストに追加する必要があります。

次に、アクセス ポイント AP001d.710d.e300 での外部 MAC アドレス フィルタリングを有効にする例を示します。

```
(Cisco Controller) >config mesh linkdata MAP2-1-1522.7400 AP001d.710d.e300 18 100 1000
30
LinkTest started on source AP, test ID: 0
[00:1D:71:0E:74:00]->[00:1D:71:0D:E3:0F]
Test config:  1000 byte packets at 100  pps for 30 seconds, a-link rate 18 Mb/s
In progress: | || || || || || || || || || || || |
```

```
LinkTest complete
Results
=======
txPkts:             2977
txBuffAllocErr:        0
txQFullErrs:           0
Total rx pkts heard at destination:      2977
rx pkts decoded correctly:               2977
  err pkts: Total         0 (PHY 0 + CRC 0 + Unknown 0), TooBig 0, TooSmall 0
  rx lost packets:        0 (incr for each pkt seq missed or out of order)
  rx dup pkts:            0
  rx out of order:        0
avgSNR:    30, high:   33, low:    3
SNR profile         [0dB...60dB]
          0            6            0            0            0
          0            0            1            2           77
       2888            3            0            0            0
          0            0            0            0            0
    (>60dB)            0
avgNf:    -95, high:  -67, low:  -97
Noise Floor profile [-100dB...-40dB]
          0         2948           19            3            1
          0            0            0            0            0
          3            3            0            0            0
          0            0            0            0            0
    (>-40dB)           0
avgRssi:   64, high:   68, low:   63
RSSI profile        [-100dB...-40dB]
          0            0            0            0            0
          0            0            0            0            0
          0            0            0            0            0
          0            0            0            0            0
    (>-40dB)        2977
Summary PktFailedRate (Total pkts sent/recvd):                       0.000%
Physical layer Error rate (Total pkts with errors/Total pkts heard): 0.000%
```

次に、アクセス ポイント AP001d.71d.e300 の外部 MAC フィルタリングを有効にする例を示します。

```
(Cisco Controller) >config mesh linkdata AP001d.710d.e300
[SD:0,0,0(0,0,0), 0,0, 0,0]
[SD:1,105,0(0,0,0),30,704,95,707]
[SD:2,103,0(0,0,0),30,46,95,25]
[SD:3,105,0(0,0,0),30,73,95,29]
[SD:4,82,0(0,0,0),30,39,95,24]
[SD:5,82,0(0,0,0),30,60,95,26]
[SD:6,105,0(0,0,0),30,47,95,23]
[SD:7,103,0(0,0,0),30,51,95,24]
[SD:8,105,0(0,0,0),30,55,95,24]
[SD:9,103,0(0,0,0),30,740,95,749]
[SD:10,105,0(0,0,0),30,39,95,20]
[SD:11,104,0(0,0,0),30,58,95,23]
[SD:12,105,0(0,0,0),30,53,95,24]
[SD:13,103,0(0,0,0),30,64,95,43]
[SD:14,105,0(0,0,0),30,54,95,27]
[SD:15,103,0(0,0,0),31,51,95,24]
[SD:16,105,0(0,0,0),30,59,95,23]
[SD:17,104,0(0,0,0),30,53,95,25]
[SD:18,105,0(0,0,0),30,773,95,777]
[SD:19,103,0(0,0,0),30,745,95,736]
[SD:20,105,0(0,0,0),30,64,95,54]
[SD:21,103,0(0,0,0),30,747,95,751]
[SD:22,105,0(0,0,0),30,55,95,25]
```

```
[SD:23,104,0(0,0,0),30,52,95,35]
[SD:24,105,0(0,0,0),30,134,95,23]
[SD:25,103,0(0,0,0),30,110,95,76]
[SD:26,105,0(0,0,0),30,791,95,788]
[SD:27,103,0(0,0,0),30,53,95,23]
[SD:28,105,0(0,0,0),30,128,95,25]
[SD:29,104,0(0,0,0),30,49,95,24]
[SD:30,0,0(0,0,0), 0,0, 0,0]
```

config mesh linktest

メッシュ アクセス ポイント間のクライアント アクセスを確認するには、**config mesh linktest** コマンドを使用します。

config mesh linktest *source_ap* {*dest_ap* | *MAC addr*} *datarate packet_rate packet_size duration*

構文の説明

source_ap	発信元アクセス ポイント。
dest_ap	宛先アクセス ポイント。
MAC addr	MAC アドレス。
datarate	• 802.11a 無線のデータ レート。有効な値は 6、9、11、12、18、24、36、48、54 Mbps です。 • 802.11b 無線のデータ レート。有効な値は、6、12、18、24、36、54、100 Mbps です。 • 802.11n 無線のデータ レート。有効な値は m0 ～ m15 間の MCS レートです。
packet_rate	パケット数/秒。有効な範囲は 1 ～ 3000 ですが、推奨されるデフォルトは 100 です。
packet_size	（任意）バイト単位のパケット サイズ。指定されていない場合、パケット サイズは 1500 バイトにデフォルト設定されます。
duration	（任意）秒単位のテスト期間。有効な値は、10 ～ 300 秒です。指定されていない場合、期間は 30 秒にデフォルト設定されます。

コマンド デフォルト

100 パケット/秒、1500 バイト、30 秒間。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config mesh linktest コマンドと **config mesh linkdata** コマンドは、同時に使用して、発信元アクセス ポイントと宛先アクセス ポイントで情報を照合するように設計されています。この情報を取得するには、まず *dest_ap* 引数でデータのリンク元になるアクセス ポイントを指定して **config mesh linktest** コマンドを入力します。このコマンドが完了して、**config mesh linkdata** コ

マンドを入力すると、同じ宛先アクセス ポイントがリスト表示され、リンク データが表示されます。

リンクをオーバーサブスクライブするおそれのあるリンクテストを実行すると、次の警告メッセージが表示されます。

```
Warning! Data Rate (100 Mbps) is not enough to perform this link test
on packet size (2000bytes) and (1000) packets per second. This may cause
AP to disconnect or reboot. Are you sure you want to continue?
```

次に、メッシュ アクセス ポイント *SB_MAP1* と *SB_RAP2*（*36 Mbps*、*20 fps*、*100* フレーム サイズ、*15* 秒間）のクライアント アクセスを確認する例を示します。

```
(Cisco Controller) >config mesh linktest SB_MAP1 SB_RAP1 36 20 100 15
LinkTest started on source AP, test ID: 0
[00:1D:71:0E:85:00]->[00:1D:71:0E:D0:0F]
Test config:  100 byte packets at 20  pps for 15 seconds, a-link rate 36 Mb/s
In progress: | || || || || || |
LinkTest complete
Results
=======
txPkts:              290
txBuffAllocErr:        0
txQFullErrs:           0
Total rx pkts heard at destination:       290
rx pkts decoded correctly:
  err pkts: Total         0 (PHY 0 + CRC 0 + Unknown 0), TooBig 0, TooSmall 0
  rx lost packets:        0 (incr for each pkt seq missed or out of order)
  rx dup pkts:            0
  rx out of order:        0
avgSNR:    37, high:   40, low:    5
SNR profile         [0dB...60dB]
          0            1            0            0            1
          3            0            1            0            2
          8           27          243            4            0
          0            0            0            0            0
    (>60dB)            0
avgNf:    -89, high:  -58, low:  -90
Noise Floor profile [-100dB...-40dB]
          0            0            0          145          126
         11            2            0            1            0
          3            0            1            0            1
          0            0            0            0            0
    (>-40dB)           0
avgRssi:   51, high:   53, low:   50
RSSI profile        [-100dB...-40dB]
          0            0            0            0            0
          0            0            0            0            0
          0            0            0            0            0
          0            7          283            0            0
    (>-40dB)           0
Summary PktFailedRate (Total pkts sent/recvd):                        0.000%
Physical layer Error rate (Total pkts with errors/Total pkts heard): 0.000%
```

次の表に、**config mesh linktest** コマンドで表示される出力フラグを示します。

表 *1 : Config Mesh Linktest* コマンドの出力フラグ

出力フラグ	説明
txPkts	ソースから送信されたパケット数。
txBuffAllocErr	発信元での linktest バッファ割り当てエラーの数（ゼロであると予想される）。
txQFullErrs	発信元での linktest キューフルエラーの数（ゼロであると予想される）。
Total rx pkts heard at destination	宛先で受信された linktest パケットの数（txPkts と同じまたは近似値であると予想される）。
rx pkts decoded correctly	宛先で受信され正しくデコードされた linktest パケットの数（txPkts と同じまたは近似値であると予想される）。
err pkts: Total	エラーのある linktest パケットのパケット エラー統計情報。
rx lost packets	宛先で受信されない linktest パケットの総数。
rx dup pkts	宛先で受信した重複 linktest パケットの総数。
rx out of order	宛先で順序が入れ替わって受信された linktest パケットの総数。
avgNF	平均ノイズ フロア。
Noise Floor profile	ノイズフロアのプロファイル（dB 単位）は負の数値です。
avgSNR	平均 SNR 値。
SNR profile [odb...60dB]	0～60 dB の間で受信したヒストグラムのサンプル。SNR プロファイルの異なる列はバケット 0-3、3-6、6-9、最大 57-60 を下回るパケット数です。
avgRSSI	平均 RSSI 値。平均の上限および下限 RSSI 値は正の数値です。
RSSI profile [-100dB...-40dB]	RSSI プロファイル（dB 単位）は負の数値です。

config mesh lsc

メッシュ アクセス ポイントのローカルで有効な証明書（LSC）を設定するには、**config mesh lsc** コマンドを使用します。

config mesh lsc {**enable** | **disable**}

構文の説明

enable	メッシュ アクセス ポイントの LSC を有効にします。
disable	メッシュ アクセス ポイントの LSC を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、メッシュ アクセス ポイントの LSC を有効にする例を示します。

```
(Cisco Controller) >config mesh lsc enable
```

config mesh lsc advanced

メッシュ アクセス ポイント（AP）の外部認証、認可、およびアカウンティング（AAA）サーバでワイルド カードが使用されている場合に高度な LSC（ローカルで有効な証明書）を設定するには、**config mesh lsc advanced** コマンドを使用します。

config mesh lsc advanced {**enable** | **disable**}

構文の説明

enable	メッシュ AP の高度な LSC を有効にします。
disable	メッシュ AP の高度な LSC を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、メッシュ AP の高度な LSC を有効にする例を示します。

```
(Cisco Controller) >config  mesh lsc advanced enable
```

config mesh lsc advanced ap-provision

メッシュアクセスポイント（AP）の外部認証、認可、およびアカウンティング（AAA）サーバでワイルドカードが使用されている場合に高度なメッシュLSC（ローカルで有効な証明書）APプロビジョニングを設定するには、**config mesh lsc advanced ap-provision** コマンドを使用します。

config mesh lsc advanced ap-provision {**enable** | **disable** | **open-window** {**enable** | **disable**} | **provision-controller** {**enable** | **disable**}}

構文の説明

enable	メッシュ AP の外部 AAA サーバでワイルド カードが使用されている場合に高度なメッシュ LSC AP プロビジョニングを有効にします。
disable	メッシュ AP の外部 AAA サーバでワイルド カードが使用されている場合に高度なメッシュ LSC AP プロビジョニングを無効にします。
open-window	MAC 検証なしですべてのメッシュ AP のメッシュ LSC プロビジョニングを設定します。
enable	MAC 検証なしですべてのメッシュ AP の AP プロビジョニングを有効にします。
disable	MAC 検証なしですべてのメッシュ AP の AP プロビジョニングを無効にします。
provision-controller	LSC を取得するためにメッシュ AP のプロビジョニング コントローラ詳細情報を設定します。
enable	LSC を取得するためのプロビジョニング コントローラ オプションを有効にします。
disable	LSC を取得するためのプロビジョニング コントローラ オプションを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、高度な AP プロビジョニング方式を有効にする例を示します。

```
(Cisco Controller) >config mesh lsc advanced ap-provision enable
```

config mesh multicast

マルチキャスト モード設定を行って、メッシュ ネットワーク内のマルチキャスト送信を管理するには、**config mesh multicast** コマンドを使用します。

config mesh multicast {**regular** | **in** | **in-out**}

構文の説明

regular	ブリッジが有効に設定されているルート アクセス ポイント（RAP）およびメッシュ アクセス ポイント（MAP）によって、メッシュ ネットワーク全体とすべてのセグメントにビデオをマルチキャストします。
in	MAP によってイーサネット マップから RAP のイーサネット ネットワークに受信されたマルチキャスト ビデオを転送します。これ以上の転送は行われないので、RAP で受信された LWAPP 以外のマルチキャストがメッシュ ネットワーク内の MAP イーサネット ネットワーク（マルチキャストの発生元）に送り返されることはありません。また、MAP-to-MAP マルチキャストは除外されているので、このようなマルチキャストは発生しません。
in-out	RAP と MAP をそれぞれを異なる方法でマルチキャストに設定します。 マルチキャスト パケットがイーサネット経由で MAP で受信された場合、RAP に送信されますが、他の MAP イーサネットには送信されません。MAP-to-MAP パケットはマルチキャストから除外されます。 マルチキャスト パケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットワークに送信されます。詳細については、「使用上のガイドライン」の項を参照してください。

コマンド デフォルト

In-out モード

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラ GUI を使用してメッシュ ネットワークのマルチキャストをイネーブルにすることはできません。

メッシュ マルチキャスト モードは、ブリッジが有効に設定されているアクセス ポイントのメッシュ アクセス ポイント（MAP）およびルート アクセス ポイント（RAP）がメッシュ ネットワーク内のイーサネット LAN 間でマルチキャストを送信する方法を決定します。メッシュ マルチキャスト モードは、LWAPP マルチキャスト以外のトラフィックだけを管理します。LWAPP マルチキャスト トラフィックは、別のメカニズムで管理されます。

コントローラ CLI を使用して 3 種類のメッシュ マルチキャスト モードを設定し、すべてのメッシュ アクセス ポイントでビデオ カメラ ブロードキャストを管理できます。イネーブルになっている場合、これらのモードは、メッシュ ネットワーク内の不要なマルチキャスト送信を減少させ、バックホール帯域幅を節約します。

in-out モードを使用する場合、ネットワークを適切に区分けして、RAP が送信したマルチキャストを同一イーサネット セグメントの別の RAP が受信し、ネットワークに送り返さないようにすることが重要です。

（注） 802.11b クライアントでの CAPWAP マルチキャストの受信が必要な場合、マルチキャストは、コントローラおよびメッシュ ネットワーク（**config network multicast global** コマンドを使用）でグローバルに有効にする必要があります。マルチキャストをメッシュ ネットワーク外の 802.11b クライアントに伝送する必要がない場合、グローバルなマルチキャスト パラメータを無効にする必要があります。

次に、ブリッジが有効に設定されている RAP および MAP によってメッシュ ネットワーク全体とすべてのセグメントにビデオをマルチキャストする例を示します。

```
(Cisco Controller) >config mesh multicast regular
```

config mesh parent preferred

メッシュ アクセス ポイントに対して優先される親を設定するには、**config mesh parent preferred** コマンドを使用します。

config mesh parent preferred *cisco_ap* {*mac_address* | **none**}

構文の説明

cisco_ap	子のアクセス ポイントの名前。
mac_address	優先される親の MAC アドレス。
none	設定された親をクリアします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

子の AP は、次の基準に基づいて優先される親を選択します。

- 優先される親は最良の親です。
- 優先される親には少なくとも 20 dB のリンク SNR があります（他の親はどんなに優れていても無視されます）。
- 優先される親には 12 dB ～ 20 dB の範囲内のリンク SNR がありますが、他の親が非常に優れていることはありません（つまり、SNR が 20 % 以上優れている）。SNR が 12 dB 未満の場合、設定は無視されます。
- 優先される親はブラックリストに掲載されません。
- 優先される親は、12 dB ～ 20 dB の範囲内の（DFS）のため、サイレント モードになりません。
- 優先される親は同じブリッジ グループ名（BGN）に属します。設定された優先される親が同じBGNに属さず、他の親が利用可能でない場合、子はデフォルトのBGNを使用して親 AP に join します。

次に、メッシュ アクセス ポイント myap1 に対して MAC アドレスが 00:21:1b:ea:36:60 である優先される親を設定する例を示します。

```
(Cisco Controller) >config mesh parent preferred myap1 00:21:1b:ea:36:60
```

次に、キーワードnoneを使用して、メッシュ アクセス ポイントmyap1に対してMAC アドレスが 00:21:1b:ea:36:60 である優先される親をクリアする例を示します。

```
(Cisco Controller) >config mesh parent preferred myap1 00:21:1b:ea:36:60 none
```

config mesh public-safety

メッシュ アクセス ポイント用に 4.9 GHz の Public Safety 帯域を有効または無効にするには、**config mesh public-safety** コマンドを使用します。

config mesh public-safety {**enable** | **disable**} {**all** | *cisco_ap* }

構文の説明

enable	4.9 GHz の Public Safety 帯域を有効にします。
disable	4.9 GHz の Public Safety 帯域を無効にします。
all	すべてのメッシュ アクセス ポイントにこのコマンドを適用します。
cisco_ap	特定のメッシュ アクセス ポイント。

コマンド デフォルト

4.9 GHz の Public Safety 帯域は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

4.9 GHz は、公共安全（Public Safety）に関わる職員に使用が制限された認可周波数帯域です。

次に、すべてのメッシュ アクセス ポイントに 4.9 GHz の Public Safety 帯域を有効にする例を示します。

```
(Cisco Controller) >config mesh public-safety enable all
4.9GHz is a licensed frequency band in -A domain for public-safety usage
 Are you sure you want to continue? (y/N) y
```

config mesh radius-server

メッシュ アクセス ポイントの外部認証を有効または無効にするには、**config mesh radius-server** コマンドを入力します。

config mesh radius-server *index* {**enable** | **disable**}

構文の説明

index	RADIUS 認証方式。オプションは次のとおりです。 • メッシュ RADIUS サーバ設定に拡張可能認証プロトコル（EAP）を指定するには、**eap** と入力します。 • メッシュ RADIUS サーバ設定に事前共有キー（PSK）を指定するには、**psk** と入力します。
enable	メッシュ アクセス ポイントの外部認証を有効にします。
disable	メッシュ アクセス ポイントの外部認証を無効にします。

コマンド デフォルト

EAP は有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、メッシュ アクセス ポイントの外部認証を有効にする例を示します。

```
(Cisco Controller) >config mesh radius-server eap enable
```

config mesh range

屋外のルート アクセス ポイント（RAP）とメッシュ アクセス ポイント（MAP）の最大範囲をグローバルに設定するには、**config mesh range** コマンドを使用します。

config mesh range ［*distance*］

構文の説明

distance	（任意）メッシュ アクセス ポイントの最大動作範囲（150～132,000 フィート）。

コマンド デフォルト

12,000 フィート。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを有効にすると、すべての屋外メッシュ アクセス ポイントがリブートします。このコマンドは、屋内アクセス ポイントには影響しません。

次に、屋外のメッシュ RAP と MAP の範囲を設定する例を示します。

```
(Cisco Controller) >config mesh range 300
Command not applicable for indoor mesh. All outdoor Mesh APs will be rebooted
Are you sure you want to start? (y/N) y
```

config mesh secondary-backhaul

メッシュ ネットワークでセカンダリ バックホールを設定するには、**config mesh secondary-backhaul** コマンドを使用します。

config mesh secondary-backhaul {**enable** [**force-same-secondary-channel**] | **disable** [**rll-retransmit** | **rll-transmit**]}

構文の説明

enable	セカンダリ バックホール設定を有効にします。
force-same-secondary- channel	（任意）セカンダリ バックホール メッシュ機能を有効にします。最初のホップ ノードをルートとするすべてのアクセス ポイントが同じセカンダリ チャネルを持ち、2 番目以降のホップでのメッシュ アクセス ポイント（MAP）に対する自動または手動チャネル割り当てを無視するように強制します。
disable	セカンダリ バックホール設定を無効にします。
rll-transmit	（任意）2 番目以降のホップで Reliable Link Layer（RLL）を使用します。
rll-retransmit	（任意）信頼性向上のために RLL の再試行回数を増やします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、断続的な干渉のためにプライマリ バックホールで送信できないトラフィックの一時的なパスとしてセカンダリ バックホール無線を使用します。

次に、セカンダリ バックホール無線を有効にし、最初のホップ ノードをルートとするすべてのアクセス ポイントが同じセカンダリ チャネルを持つように強制する例を示します。

```
(Cisco Controller) >config mesh secondary-backhaul enable force-same-secondary-channel
```

config mesh security

メッシュ ネットワークのセキュリティ設定を行うには、**config mesh security** コマンドを使用します。

config mesh security {{**rad-mac-filter** | **force-ext-auth** | **lsc-only-auth**} {**enable** | **disable**}} | {{**eap** | **psk provisioning** | **provisioning window**} | {**enable** | **disable**}} | {**delete_psk** | **key**}

構文の説明

rad-mac-filter	メッシュ セキュリティ設定のリモート認証ダイヤルイン ユーザ サービス（RADIUS）MAC アドレス フィルタを有効にします。
force-ext-auth	メッシュ セキュリティ設定の強制外部認証を無効にします。
lsc-only-auth	メッシュ セキュリティ設定の LSC（ローカルで有効な証明書）のみの認証を有効にします。
enable	メッシュ セキュリティ設定を有効にします。
disable	メッシュ セキュリティ設定を無効にします。
eap	メッシュ セキュリティ設定に拡張可能認証プロトコル（EAP）をデフォルトで指定します。
psk	メッシュ セキュリティ設定に事前共有キー（PSK）を指定します。
provisioning	シスコ ワイヤレス コントローラ（WLC）で PSK のプロビジョニングを暗号化します。
provisioning window	Cisco WLC で PSK のプロビジョニング ウィンドウを暗号化します。
enable	PSK のプロビジョニングを有効にします。
disable	PSK のプロビジョニングを無効にします。
key	PSK のキーを指定します。

コマンド デフォルト

メッシュ セキュリティについては EAP がデフォルトとして指定されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.2	このコマンドが変更され、PSK プロビジョニングと PSK プロビジョニング キーワードが追加されました。

次に、すべてのメッシュ アクセス ポイントのセキュリティ オプションとして EAP を設定する例を示します。

```
(Cisco Controller) config mesh security eap
```

次に、すべてのメッシュ アクセス ポイントのセキュリティ オプションとして PSK を設定する例を示します。

```
(Cisco Controller) config mesh security psk
```

次に、すべてのメッシュ アクセス ポイントのセキュリティ オプションとして PSK プロビジョニングを有効にする例を示します。

```
(Cisco Controller)> config mesh security psk provisioning enable
```

次に、すべてのメッシュ アクセス ポイントのセキュリティ オプションとして PSK プロビジョニング キーを設定する例を示します。

```
(Cisco Controller)> config mesh security psk provisioning key 5
```

次に、すべてのメッシュ アクセス ポイントのセキュリティ オプションとして PSK プロビジョニング ウィンドウを有効にする例を示します。

```
(Cisco Controller)> config mesh security psk provisioning window enable
```

次に、Cisco WLC の PSK プロビジョニングを削除する例を示します。

```
(Cisco Controller)> config mesh security psk provisioning delete_psk wlc
```

次に、すべてのメッシュ アクセス ポイントの PSK プロビジョニングを削除する例を示します。

```
(Cisco Controller)> config mesh security psk provisioning delete_psk ap
```

次に、Cisco WLC のすべての設定から PSK プロビジョニングを削除する例を示します。

```
(Cisco Controller)> config mesh security psk provisioning delete_psk wlc all
```

config mesh slot-bias

シリアルバックホールメッシュアクセスポイントのスロットバイアスを有効または無効にするには、**config mesh slot-bias** コマンドを使用します。

config mesh slot-bias {**enable** | **disable**}

構文の説明

enable	シリアル バックホール メッシュ AP のスロット バイアスを有効にします。
disable	シリアル バックホール メッシュ AP のスロット バイアスを無効にします。

コマンド デフォルト

デフォルトでは、スロット バイアスが有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用する場合、次のガイドラインに従ってください。

- **config mesh slot-bias** コマンドはグローバル コマンドであるため、同じコントローラにアソシエートされたすべての 1524SB AP に適用できます。
- スロットバイアスは、スロット1とスロット2の両方が使用可能である場合にのみ適用できます。動的周波数選択（DFS）のため、スロット無線に利用可能なチャネルがない場合は、他のスロットがアップリンクとダウンリンク両方の役割を担います。
- ハードウェアの問題のため、スロット2が利用可能でない場合でも、スロットバイアスは通常どおり機能します。スロットバイアスを無効にするか、アンテナを修復して是正処置を実行する必要があります。

次に、シリアルバックホールメッシュ AP のスロットバイアスを無効にする例を示します。

```
(Cisco Controller) >config mesh slot-bias disable
```

config mgmtuser add

コントローラにローカル管理ユーザを追加するには、**config mgmtuser add** コマンドを使用します。

config mgmtuser add *username password* {**lobby-admin** | **read-write** | **read-only**} [*description*]

構文の説明

username	アカウントユーザ名。ユーザ名には、最大24文字の英数字を使用できます。
password	アカウント パスワード。パスワードには、最大 24 文字の英数字を使用できます。
lobby-admin	ロビー アンバサダー権限を持つ管理ユーザを作成します。
read-write	読み取りと書き込みアクセス権を持つ管理ユーザを作成します。
read-only	読み取り専用アクセス権を持つ管理ユーザを作成します。
description	（任意）アカウントについての説明。説明には、最大32文字の英数字を使用できます。説明は二重引用符で囲みます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。
8.4	このコマンドにより、ロビー管理者ユーザが作成されます。

次に、読み取りと書き込みアクセス権を持つ管理ユーザアカウントを作成する例を示します。

```
(Cisco Controller) > config mgmtuser add admin admin read-write "Main account"
```

関連コマンド

show mgmtuser

config mgmtuser delete

コントローラからローカル管理ユーザを削除するには、**config mgmtuser delete** コマンドを使用します。

config mgmtuser delete *username*

構文の説明

username	アカウントユーザ名。ユーザ名には、最大24文字の英数字を使用できます。

コマンド デフォルト

管理ユーザは、デフォルトでは削除されません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、コントローラから管理ユーザ アカウントの管理者を削除する例を示します。

```
(Cisco Controller) > config mgmtuser delete admin
Deleted user admin
```

関連コマンド

show mgmtuser

config mgmtuser description

コントローラの既存の管理ユーザ ログインに説明を追加するには、**config mgmtuser description** コマンドを使用します。

config mgmtuser description *username description*

構文の説明

username	アカウントユーザ名。ユーザ名には、最大24文字の英数字を使用できます。
description	アカウントの説明。説明には、最大32文字の英数字を使用できます。説明は二重引用符で囲みます。

コマンド デフォルト

管理ユーザに説明が追加されません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、管理ユーザ「admin」に説明「master-user」を追加する例を示します。

```
(Cisco Controller) > config mgmtuser description admin "master user"
```

関連コマンド

config mgmtuser add

config mgmtuser delete

config mgmtuser password

show mgmtuser

config mgmtuser password

管理ユーザ パスワードを設定するには、**config mgmtuser password** コマンドを使用します。

config mgmtuser password *username password*

構文の説明

username	アカウントユーザ名。ユーザ名には、最大24文字の英数字を使用できます。
password	アカウント パスワード。パスワードには、最大 24 文字の英数字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、新しいパスワード5rTfmを使用して、管理ユーザ「admin」のパスワードを変更する例を示します。

```
(Cisco Controller) > config mgmtuser password admin 5rTfm
```

関連コマンド

show mgmtuser

config mgmtuser telnet

ローカル管理ユーザによる Cisco ワイヤレス LAN コントローラへの接続での Telnet を使用を有効にするには、**config mgmtuser telnet** コマンドを使用します。

config mgmtuser telnet *user_name* {**enable** | **disable**}

構文の説明

user_name	ローカル管理ユーザのユーザ名。
enable	ローカル管理ユーザによる Cisco WLC への接続での Telnet の使用を有効にします。最大 24 文字の英数字を入力できます。
disable	ローカル管理ユーザによる Cisco WLC への接続での Telnet の使用を無効にします。

コマンド デフォルト

ローカル管理ユーザは Telnet を使用して Cisco WLC に接続できます。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

このコマンドを有効にするにはグローバル Telnet を有効にする必要があります。このオプションを有効にしてもセキュア シェル（SSH）接続は影響を受けません。

次に、ローカル管理ユーザによる Cisco WLC への接続での Telnet の使用を有効にする例を示します。

```
(Cisco Controller) > config mgmtuser telnet admin1 enable
```

config mgmtuser termination-interval

ユーザの再認証終了間隔 (秒単位) を設定するには、**config mgmtuser termination-interval** コマンドを使用します。

config mgmtuser termination-interval {*seconds* }

構文の説明

seconds	ユーザがログアウトするまでの再認証終了間隔（秒単位）。デフォルト値は 0、有効な範囲は 0 ～ 300 秒です。

コマンド履歴

リリース	変更内容
8.2	このコマンドは本リリースで追加されました。

次に、ユーザがログアウトするまでの間隔（秒単位）を設定する例を示します。

```
(Cisco Controller) > config mgmtuser termination-interval 180
```

config mobility dscp

モビリティ コントローラ間の DSCP 値を設定するには、**config mobility dscp** コマンドを使用します。

config mobility dscp *dscp_value*

構文の説明

dscp_value	0～63 の DSCP 値。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、モビリティ コントローラ間の DSCP 値を 40 に設定する例を示します。

```
(Cisco Controller) >config mobility dscp 40
```

config mobility group anchor

WLAN または有線ゲスト LAN の新しいモビリティ アンカーを作成するには、**config mobility group anchor** コマンドを使用します。

config mobility group anchor {**add** | **delete**} {**wlan** *wlan_id* | **guest-lan** *guest_lan_id*} *anchor_ip*

構文の説明

add	無線 LAN にモビリティ アンカーを追加または変更します。
delete	無線 LAN からモビリティ アンカーを削除します。
wlan	無線 LAN のアンカー設定を指定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
guest-lan	ゲスト LAN のアンカー設定を指定します。
guest_lan_id	1 ～ 5 のゲスト LAN 識別子。
anchor_ip	アンカー コントローラの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

wlan_id または *guest_lan_id* は必ず指定し、無効にする必要があります。

1 つ目のモビリティ アンカーを設定するときに、WLAN または有線ゲスト LAN で自動アンカー モビリティを有効にします。最後のアンカーを削除すると、自動アンカー モビリティ機能は無効になり、新しいアソシエーションに対しては標準のモビリティが再度使用されるようになります。

次に、無線 LAN ID 2 に IP アドレス 192.12.1.5 のモビリティ アンカーを追加する例を示します。

```
(Cisco Controller) >config mobility group anchor add wlan 2 192.12.1.5
```

次に、無線 LAN から IP アドレス 193.13.1.15 のモビリティ アンカーを削除する例を示します。

```
(Cisco Controller) >config mobility group anchor delete wlan 5 193.13.1.5
```

config mobility group domain

モビリティ ドメイン名を設定するには、**config mobility group domain** コマンドを使用します。

config mobility group domain *domain_name*

構文の説明

domain_name	ドメイン名。ドメイン名は最大31文字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、モビリティ ドメイン名 lab1 を設定する例を示します。

```
(Cisco Controller) >config mobility group domain lab1
```

config mobility group keepalive count

エラーが発生したモビリティ グループ メンバー（アンカー Cisco WLC を含む）を検出するように Cisco WLC を設定するには、**config mobility group keepalive count** コマンドを使用します。

config mobility group keepalive count *count*

構文の説明

count	モビリティ グループ メンバーに ping 要求を送信する回数。この回数を超えると、メンバーにはアクセスできないと見なされます。有効な範囲は 3 ～ 20 です。デフォルトは 3 です。

コマンド デフォルト

モビリティ グループ メンバーに ping 要求を送信するデフォルトの回数は 3 回です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、モビリティ グループ メンバーに ping 要求を送信する回数を 3 回に指定する方法の例を示します。この回数を超えると、メンバーにはアクセスできないと見なされます。

```
(Cisco Controller) >config mobility group keepalive count 3
```

config mobility group keepalive interval

エラーが発生したモビリティ グループ メンバー（アンカー コントローラを含む）を検出するようにコントローラを設定するには、**config mobility group keepalive** コマンドを使用します。

config mobility group keepalive *interval*

構文の説明

interval	モビリティ グループ メンバーへの ping 要求の送信間隔。範囲は 1 ～ 30 秒です。デフォルト値は 10 秒です。

コマンド デフォルト

ping 要求のデフォルトの送信間隔は 10 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、モビリティ グループ メンバーに ping 要求を送信する間隔を 10 秒に指定する例を示します。

```
(Cisco Controller) >config mobility group keepalive 10
```

config mobility group member

モビリティ グループのメンバー リストのユーザを追加または削除するには、**config mobility group member** コマンドを使用します。

config mobility group member {**add** *MAC-addr IP-addr* [*group_name*] | **delete** *MAC-addr* | **hash** *IP-addr* {*key* | **none**}}

構文の説明

add	リストのモビリティ グループ メンバーを追加または変更します。
mac-addr	メンバー スイッチの MAC アドレス。
IP-addr	メンバー スイッチの IP アドレス。
group_name	（任意）メンバー スイッチ グループ名（デフォルトのグループ名と異なる場合）。
delete	（任意）リストからモビリティ グループ メンバーを削除します。
hash	認証のためにハッシュ キーを設定します。メンバーが同じ仮想ドメインのコントローラである場合だけ、ハッシュ キーを設定できます。
key	仮想コントローラのハッシュ キー。たとえば、a819d479dcfeb3e0974421b6e8335582263d9169 のようになります。
none	仮想コントローラの以前のハッシュ キーをクリアします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、IPv4 アドレスを持つモビリティ グループ メンバーをリストに追加する例を示します。

```
(Cisco Controller) >config mobility group member add 11:11:11:11:11:11 209.165.200.225
```

次に、IPv6アドレスを持つモビリティ グループ メンバーをリストに追加する例を示します。

```
(Cisco Controller) >config mobility group member add 11:11:11:11:11:11 2001:DB8::1
```

次に、同じドメインの仮想コントローラのハッシュ キーを設定する例を示します。

（注） この例の IP アドレスには、IPv4 または IPv6 のいずれかの形式を使用できます。

```
(Cisco Controller) >config mobility group member hash 209.165.201.1
a819d479dcfeb3e0974421b6e8335582263d9169
```

config mobility group multicast-address

モビリティ リスト内の非ローカル グループに対して、マルチキャスト グループ IP アドレスを設定するには、**config mobility group multicast-address** コマンドを使用します。

config mobility group multicast-address *group_name ip_address*

構文の説明

group_name	メンバ スイッチ グループ名（デフォルトのグループ名と異なる場合）。
ip_address	メンバ スイッチの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、test という名前のグループに対して、マルチキャスト グループの IP アドレス 10.10.10.1 を設定する例を示します。

```
(Cisco Controller) >config mobility group multicast-address test 10.10.10.1
```

次に、test という名前のグループに対して、マルチキャスト グループの IP アドレス 2001:DB8::1 を設定する例を示します。

```
(Cisco Controller) >config mobility group multicast-address test 2001:DB8::1
```

config mobility multicast-mode

モビリティ マルチキャスト モードを有効または無効にするには、**config mobility multicast-mode** コマンドを使用します。

config mobility multicast-mode {**enable** | **disable**} *local_group_multicast_address*

構文の説明

enable	マルチキャストモードをイネーブルにします。この場合、コントローラはマルチキャストモードを使用して、Mobile Announce メッセージをローカル グループへ送信します。
disable	マルチキャスト モードをディセーブルにします。この場合、コントローラはユニキャストモードを使用して、Mobile Announce メッセージをローカル グループへ送信します。
local_group_multicast_address	ローカル モビリティ グループの IP アドレス。

コマンド デフォルト

モビリティ マルチキャスト モードは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ローカル モビリティ グループの IP アドレス 157.168.20.0 に対して、マルチキャスト モビリティ モードを有効にする例を示します。

```
(Cisco Controller) >config mobility multicast-mode enable 157.168.20.0
```

config mobility new-architecture

Cisco ワイヤレス LAN コントローラ（WLC） で新しいモビリティを有効にするには、**config mobility new-architecture** コマンドを使用します。

config mobility new-architecture {**enable** | **disable**}

構文の説明

enable	新しいモビリティ アーキテクチャに切り替えるように Cisco WLC を設定します。
disable	古いフラット モビリティ アーキテクチャに切り替えるように Cisco WLC を設定します。

コマンド デフォルト

デフォルトでは、新しいモビリティは無効になっています。

コマンド履歴

リリース	変更内容
7.3.112.0	このコマンドが導入されました。

使用上のガイドライン

新しいモビリティは、Cisco WiSM2、Cisco 2500 シリーズ ワイヤレス コントローラ、Cisco 5500 シリーズ ワイヤレス コントローラ、および Cisco 8500 シリーズ ワイヤレス コントローラでのみサポートされています。新しいモビリティは、Cisco Catalyst 3850 シリーズや Cisco 5760 ワイヤレス LAN コントローラなどのワイヤレス コントロール モジュール（WCM）を使用した統合アクセス コントローラとの互換性を Cisco WLC で実現します。

次に、Cisco WLC で新しいモビリティを有効にする例を示します。

```
(Cisco Controller) >config mobility new-architecture enable
```

config mobility oracle

Mobility Oracle（MO）を設定するには、**config mobility oracle** コマンドを使用します。

config mobility oracle {**enable** | **disable** | **ip** *ip_address* }

構文の説明

enable	起動時に MO を有効にします。
disable	起動時に MO を無効にします。
ip	MO の IP アドレスを指定します。
ip_address	MO の IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.3.112.0	このコマンドが導入されました。
8.0	このコマンドは、IPv4アドレス形式のみをサポートします。

使用上のガイドライン

MO は 1 つの完全なモビリティ ドメインの下で、クライアント データベースを保持します。これは、ステーション データベース、モビリティ Cisco WLC へのインターフェイス、および NTP サーバで構成されます。モビリティ ドメイン全体に MO は 1 つのみです。

このコマンドでは IPv6 アドレス形式はサポートされません。

次に、MO の IP アドレスを設定する例を示します。

```
(Cisco Controller) >config mobility oracle ip 27.0.0.1
```

config mobility secure-mode

Cisco WLC 間でやり取りするモビリティ メッセージにセキュア モードを設定するには、**config mobility secure-mode** コマンドを使用します。

config mobility secure-mode {**enable** | **disable**}

構文の説明

enable	モビリティ グループのメッセージ セキュリティをイネーブルにします。
disable	モビリティ グループのメッセージ セキュリティをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、モビリティ メッセージのセキュア モードを有効にする例を示します。

```
(Cisco Controller) >config mobility secure-mode enable
```

config mobility statistics reset

モビリティの統計情報をリセットするには、**config mobility statistics reset** コマンドを使用します。

config mobility statistics reset

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、モビリティ グループの統計情報をリセットする例を示します。

```
(Cisco Controller) >config mobility statistics reset
```

config netuser add

コントローラ上のローカルユーザデータベースにWLAN上のゲストユーザまたは有線ゲストLANを追加するには、**config netuser add** コマンドを使用します。

config netuser add *username password* {**wlan** *wlan_id* | **guestlan** *guestlan_id*} **userType guest lifetime** *lifetime* **description** *description*

構文の説明

username	ゲストユーザ名。ユーザ名には、最大50文字の英数字を使用できます。
password	ユーザパスワード。パスワードには、最大24文字の英数字を使用できます。
wlan	関連付ける無線LANの識別子を指定するか、すべての無線 LAN にゼロを指定します。
wlan_id	ユーザに割り当てられている無線 LAN 識別子。値 0 の場合、ユーザをすべての無線 LAN にアソシエートします。
guestlan	関連付けるゲスト LAN の識別子を指定するか、すべての無線LANにゼロを指定します。
guestlan_id	ゲスト LAN の ID。
userType	ユーザ タイプを指定します。
guest	ゲスト ユーザのゲストを指定します。
lifetime	ライフタイムを指定します。
lifetime	ゲスト ユーザの秒単位のライフタイム値（60 ～ 259200 または 0）。 （注） 値 0 は、ライフタイム値が無制限であることを示します。
description	ユーザの簡単な説明。説明は二重引用符で囲み、最大 32 文字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

ローカル ネットワーク ユーザは 1 つのデータベースに格納されるので、これらのユーザ名は重複してはいけません。

次に、永久ユーザ名 Jane をワイヤレス ネットワークに 1 時間追加する例を示します。

```
(Cisco Controller) > config netuser add jane able2 1 wlan_id 1 userType permanent
```

次に、ゲスト ユーザ名 George をワイヤレス ネットワークに 1 時間追加する例を示します。

```
(Cisco Controller) > config netuser add george able1 guestlan 1 3600
```

関連コマンド

show netuser

config netuser delete

config netuser delete

ローカル ネットワークから既存のユーザを削除するには、**config netuser delete** コマンドを使用します。

config netuser delete { **username** *username* | **wlan-id** *wlan-id*}

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、最大 24 文字の英数字を使用できます。
wlan-id	WLAN ID 番号。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ローカル ネットワーク ユーザは 1 つのデータベースに格納されるので、これらのユーザ名は重複してはいけません。

（注） ネットワーク ユーザに関連付けられている WLAN を削除すると、システムは、先に WLAN に関連付けられているすべてのネットワーク ユーザを削除するように指示するプロンプトを表示します。ネットワーク ユーザを削除した後に、WLAN を削除できます。

次に、既存のユーザ名 able1 をネットワークから削除する例を示します。

```
(Cisco Controller) > config netuser delete able1
Deleted user able1
```

関連コマンド

show netuser

config netuser description

既存のネットワーク ユーザに説明を追加するには、**config netuser description** コマンドを使用します。

config netuser description *username description*

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、最大 24 文字の英数字を使用できます。
description	（任意）ユーザの説明。説明は二重引用符で囲み、最大 32 文字の英数字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ユーザの説明「HQ1 Contact」を既存のネットワーク ユーザ名 able 1 に追加する例を示します。

```
(Cisco Controller) > config netuser description able1 "HQ1 Contact"
```

関連コマンド

show netuser

config network dns serverip

ネットワークの DNS サーバを設定するには、**config network dns serverip** コマンドを使用します。

config network dns serverip { *ipaddr*}

構文の説明

ipaddr	IP アドレスを指定します。

コマンド デフォルト

ネットワーク レベルの Web 認証のデフォルト値は無効になっています。

コマンド履歴

リリース	変更内容
8.3	このコマンドが追加されました。

次に、Web 認証クライアントのプロキシのリダイレクションのサポートを有効にする例を示します。

```
cisco controller config network dns serverip 198.172.202.252
```

関連コマンド

show network summary

config netuser guest-lan-id

ネットワーク ユーザの有線ゲスト LAN ID を設定するには、**config netuser guest-lan-id** コマンドを使用します。

config netuser guest-lan-id *username lan_id*

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、24 文字の英数字を指定できます。
lan_id	ユーザと関連付けるための有線ゲスト LAN の ID。値が 0 の場合、ユーザはすべての有線 LAN に関連付けられます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、有線 LAN ID 2 を aire1 という名前のユーザに関連付けるように設定する例を示します。

```
(Cisco Controller) > config netuser guest- lan-id aire1 2
```

関連コマンド

show netuser

show wlan summary

config netuser guest-role apply

ゲスト ユーザに Quality of Service（QoS）のロールを適用するには、**config netuser guest-role apply** コマンドを使用します。

config netuser guest-role apply *username role_name*

構文の説明

username	ユーザ名。
role_name	QoS ゲスト ロール名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ゲスト ユーザに QoS ロールを割り当てない場合、[User Details] の [Role] フィールドにデフォルトとしてロールが示されます。このユーザの帯域幅コントラクトは、WLAN の QoS プロファイルで定義されます。

ゲスト ユーザの QoS ロールの割り当てを解除する場合は、**config netuser guest-role apply** *username* **default** を使用します。今後、このユーザについては WLAN の QoS プロファイルで定義された帯域幅コントラクトが使用されます。

次に、Contractor という名前の QoS ゲスト ロールを持つゲスト ユーザ jsmith QoS ロールを適用する例を示します。

```
(Cisco Controller) > config netuser guest-role apply jsmith Contractor
```

関連コマンド

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role create

ゲストユーザの Quality of Service（QoS）ロールを作成するには、**config netuser guest-role create** コマンドを使用します。

config netuser guest-role create *role_name*

構文の説明

role name	QoS ゲスト ロール名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

QoS ロールを削除するには、**config netuser guest-role delete** *role-name* を使用します。

次に、guestuser1 という名前のゲスト ユーザに QoS ロールを作成する例を示します。

```
(Cisco Controller) > config netuser guest-role create guestuser1
```

関連コマンド

config netuser guest-role delete

config netuser guest-role delete

ゲスト ユーザの Quality of Service（QoS）のロールを削除するには、**config netuser guest-role delete** コマンドを使用します。

config netuser guest-role delete *role_name*

構文の説明

role name	Quality of Service（QoS）ゲスト ロール名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、guestuser1 の Quality of Service（QoS）のロールを削除する例を示します。

```
(Cisco Controller) > config netuser guest-role delete guestuser1
```

関連コマンド

config netuser guest-role create

config netuser guest-role qos data-rate average-data-rate

ユーザ 1 人あたりの TCP トラフィックの平均データ レートを設定するには、**config netuser guest-role qos data-rate average-data-rate** コマンドを使用します。

config netuser guest-role qos data-rate average-data-rate *role_name rate*

構文の説明

role_name	Quality of Service（QoS）ゲスト ロール名。
rate	ユーザ 1 人あたりの TCP トラフィック レート。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドの *role_name* パラメータには、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意に識別するものです（contractor、vendor など）。*rate* パラメータには、0 ～ 60,000 Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

次に、guestuser1 という名前の QoS ゲストの平均レートを設定する例を示します。

```
(Cisco Controller) > config netuser guest-role qos data-rate average-data-rate guestuser1
 0
```

関連コマンド

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role qos data-rate burst-data-rate

config netuser guest-role qos data-rate average-realtime-rate

ユーザ 1 人あたりの TCP トラフィックの平均データ レートを設定するには、**config netuser guest-role qos data-rate average-realtime-rate** コマンドを使用します。

config netuser guest-role qos data-rate average-realtime-rate *role_name rate*

構文の説明

role_name	Quality of Service（QoS）ゲスト ロール名。
rate	ユーザ 1 人あたりの TCP トラフィック レート。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドの *role_name* パラメータには、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意に識別するものです（contractor、vendor など）。*rate* パラメータには、0 ～ 60,000 Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

次に、TCP トラフィックのレートが 0 Kbps である guestuser1 という名前の QoS ゲスト ユーザに対して平均データ レートを設定する例を示します。

```
(Cisco Controller) > config netuser guest-role qos data-rate average-realtime-rate
guestuser1 0
```

関連コマンド

config netuser guest-role

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-data-rate

ユーザ 1 人あたりの TCP トラフィックの最大データ レートを設定するには、**config netuser guest-role qos data-rate burst-data-rate** コマンドを使用します。

config netuser guest-role qos data-rate burst-data-rate *role_name rate*

構文の説明

role_name	Quality of Service（QoS）ゲスト ロール名。
rate	ユーザ 1 人あたりの TCP トラフィック レート。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

バースト データ レートは平均データ レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

このコマンドの *role_name* パラメータには、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意に識別するものです（contractor、vendor など）。*rate* パラメータには、0 ～ 60,000 Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

次に、TCP トラフィックのレートが 0 Kbps である guestuser1 という名前の QoS ゲスト に対してピーク データ レートを設定する例を示します。

```
(Cisco Controller) > config netuser guest-role qos data-rate burst-data-rate guestuser1
 0
```

関連コマンド

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-realtime-rate

ユーザ 1 人あたりの UDP トラフィックのバースト リアルタイム データ レートを設定するには、**config netuser guest-role qos data-rate burst-realtime-rate** コマンドを使用します。

config netuser guest-role qos data-rate burst-realtime-rate *role_name rate*

構文の説明

role_name	Quality of Service（QoS）ゲスト ロール名。
rate	ユーザ 1 人あたりの TCP トラフィック レート。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

バースト リアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、Quality of Service（QoS）ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

このコマンドの *role_name* パラメータには、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意に識別するものです（contractor、vendor など）。*rate* パラメータには、0 ～ 60,000 Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

次に、TCP トラフィックのレートが 0 Kbps である guestuser1 という名前の QoS ゲスト ユーザに対してバースト リアルタイム レートを設定する例を示します。

```
(Cisco Controller) > config netuser guest-role qos data-rate burst-realtime-rate guestuser1
0
```

関連コマンド

config netuser guest-role

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-data-rate

config netuser lifetime

ゲスト ネットワーク ユーザのライフタイムを設定するには、**config netuser lifetime** コマンドを使用します。

config netuser lifetime *username time*

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、最大 50 文字の英数字を使用できます。
time	60 ～ 31536000 秒のライフタイム、または制限なしの場合は 0。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ゲストのネットワーク ユーザのライフタイムを設定する例を示します。

```
(Cisco Controller) > config netuser lifetime guestuser1 22450
```

関連コマンド

show netuser

show wlan summary

config netuser maxUserLogin

ネットワーク ユーザが利用できるログインセッションの最大数を設定するには、**config netuser maxUserLogin** コマンドを使用します。

config netuser maxUserLogin *count*

構文の説明

count	単一ユーザの最大ログイン セッション数。指定できる値は 0（無制限）～ 8 です。

コマンド デフォルト

デフォルトでは、単一ユーザの最大ログイン セッション数は 0（無制限）です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、単一のユーザのログイン セッションの最大回数を 8 に設定する例を示します。

```
(Cisco Controller) > config netuser maxUserLogin 8
```

関連コマンド

show netuser

config netuser password

ローカル ネットワーク ユーザのパスワードを変更するには、**config netuser password** コマンドを使用します。

config netuser password *username password*

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、最大 24 文字の英数字を使用できます。
password	ネットワーク ユーザ パスワード。パスワードには、最大 24 文字の英数字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、aire1 から aire2 にネットワーク ユーザ パスワードを変更する例を示します。

```
(Cisco Controller) > config netuser password aire1 aire2
```

関連コマンド

show netuser

config netuser wlan-id

ネットワーク ユーザの無線 LAN ID を設定するには、**config netuser wlan-id** コマンドを使用します。

config netuser wlan-id *username wlan_id*

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、24 文字の英数字を指定できます。
wlan_id	ユーザとアソシエートする無線LAN識別子。値 0 の場合、ユーザをすべての無線 LAN にアソシエートします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

例

次に、無線 LAN ID 2 を aire1 という名前のユーザに関連付けるように設定する例を示します。

```
(Cisco Controller) > config netuser wlan-id aire1 2
```

関連コマンド

show netuser

show wlan summary

config network client-ip-conflict-detection

ネットワークのクライアント DHCP アドレス競合検出を有効または無効にするには、**config network client-ip-conflict-detection** コマンドを使用します。

config network client-ip-conflict-detection {**enable** | **disable**}

構文の説明

enable	ワイヤレス クライアントが、すでに別のクライアントに登録されている DHCP アドレスを受信した場合、以前のクライアントは切断されるため、そのクライアントは再接続して新しいアドレスを取得する必要があります。
disable	この機能をディセーブルにします。

コマンド デフォルト

ディセーブル

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

config network http-proxy ip-address

ネットワークのHTTPプロキシサーバのIPアドレスを設定するには、**config network http-proxy ip-address** コマンドを使用します。

config network http-proxy ip-address *ip-address* **port** *port-no*

構文の説明

ip-address	HTTP プロキシの IP アドレス。
port-no	HTTP プロキシのポート番号。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.3	このコマンドが導入されました。

次に、ネットワークのHTTPプロキシサーバのIPアドレスを設定する例を示します。

```
cisco controller config network http-proxy ip-address 10.10.10.11 port 8080
```

関連コマンド

show network summary

config network bridging-shared-secret

ブリッジの共有キーを設定するには、**config network bridging-shared-secret** コマンドを使用します。

config network bridging-shared-secret *shared_secret*

構文の説明

shared_secret	ブリッジの共有キーの文字列。文字列には 10 バイトまで使用できます。

コマンド デフォルト

ブリッジの共有キーは、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドにより、スイッチに接続するメッシュ アクセス ポイントのバックホール ユーザ データを暗号化する共有キーが作成されます。

このコマンドを機能させるには、zero touch configuration をイネーブルにしておく必要があります。

次に、ブリッジの共有キーの文字列「shhh1」を設定する例を示します。

```
(Cisco Controller) > config network bridging-shared-secret shhh1
```

関連コマンド

show network summary

config network web-auth captive-bypass

ネットワーク レベルでキャプティブ ポータルのバイパスをサポートするようにコントローラを設定するには、**config network web-auth captive-bypass** コマンドを使用します。

config network web-auth captive-bypass {**enable** | **disable**}

構文の説明

enable	コントローラがキャプティブ ポータルのバイパスをサポートできるようにします。
disable	コントローラがキャプティブ ポータルのバイパスをサポートできないようにします。

コマンド デフォルト

なし

次に、キャプティブ ポータルのバイパスをサポートするようにコントローラを設定する例を示します。

```
(Cisco Controller) > config network web-auth captive-bypass enable
```

関連コマンド

show network summary

config network web-auth cmcc-support

config network web-auth port

ネットワーク レベルの Web 認証に関して追加ポートがリダイレクトされるように設定するには、**config network web-auth port** コマンドを使用します。

config network web-auth port *port*

構文の説明

port	ポート番号。有効な範囲は 0 ～ 65535 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、Web認証に関して、追加ポート番号1200がリダイレクトされるように設定する例を示します。

```
(Cisco Controller) > config network web-auth port 1200
```

関連コマンド

show network summary

config network web-auth proxy-redirect

Web認証クライアントのプロキシのリダイレクションサポートを設定するには、**config network web-auth proxy-redirect** コマンドを使用します。

config network web-auth proxy-redirect {**enable** | **disable**}

構文の説明

enable	Web 認証クライアントのプロキシ リダイレクションをサポートできるようにします。
disable	Web 認証クライアントのプロキシ リダイレクションをサポートできないようにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web 認証クライアントのプロキシのリダイレクションのサポートを有効にする例を示します。

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

関連コマンド

show network summary

config network web-auth secureweb

クライアントにセキュア Web（https）認証を設定するには、**config network web-auth secureweb** コマンドを使用します。

config network web-auth secureweb {**enable** | **disable**}

構文の説明

enable	クライアントにセキュア Web（https）認証を行えるようにします。
disable	クライアントにセキュア Web（https）認証を行えないようにします。クライアントのHTTP Web 認証を有効にします。

コマンド デフォルト

デフォルトでは、クライアントのセキュア Web（https）認証は有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

config network web-auth secureweb disable コマンドを使用してクライアントのセキュア Web（https）認証を設定する場合、Cisco WLC をリブートして変更を適用する必要があります。

次に、クライアントに対してセキュア Web（https）認証を有効にする例を示します。

```
(Cisco Controller) > config network web-auth secureweb enable
```

関連コマンド

show network summary

config network webmode

Web モードを有効または無効にするには、**config network webmode** コマンドを使用します。

config network webmode {**enable** | **disable**}

構文の説明

enable	Webインターフェイスをイネーブルにします。
disable	Web インターフェイスをディセーブルにします。

コマンド デフォルト

Web モードのデフォルト値は **enable** です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web インターフェイス モードを無効にする例を示します。

```
(Cisco Controller) > config network webmode disable
```

関連コマンド

show network summary

config network web-auth

ネットワーク レベルの Web 認証オプションを設定するには、**config network web-auth** コマンドを使用します。

config network web-auth {**port** *port-number*} | {**proxy-redirect** {**enable** | **disable**}}

構文の説明

port	Web 認証リダイレクション用に追加ポートを設定します。
port-number	ポート番号（0 ～ 65535）。
proxy-redirect	Web 認証クライアントのプロキシ リダイレクション サポートを設定します。
enable	Web 認証クライアントのプロキシ リダイレクション サポートをイネーブルにします。 （注） Web 認証プロキシのリダイレクションは、ポート 80、8080、および 3128 に加え、ユーザ定義のポート 345 に対してイネーブルになります。
disable	Web 認証クライアントのプロキシ リダイレクション サポートをディセーブルにします。

コマンド デフォルト

ネットワーク レベルの Web 認証のデフォルト値は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

設定を有効にするには、システムをリセットする必要があります。

次に、Web 認証クライアントのプロキシのリダイレクションのサポートを有効にする例を示します。

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

関連コマンド

show network summary

show run-config

config qos protocol-type

config network 802.3-bridging

コントローラで 802.3 ブリッジを有効または無効にするには、**config network 802.3-bridging** コマンドを使用します。

config network 802.3-bridging {**enable** | **disable**}

構文の説明

enable	802.3 ブリッジをイネーブルにします。
disable	802.3 ブリッジをディセーブルにします。

コマンド デフォルト

デフォルトでは、コントローラで 802.3 ブリッジが無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラ ソフトウェア リリース 5.2 では、2100 シリーズベース コントローラ用のソフトウェアベースのフォワーディング アーキテクチャが新しいフォワーディング プレーン アーキテクチャになります。その結果、2100 シリーズ コントローラおよび Cisco サービス統合型ルータ用 Cisco Wireless LAN Controller Network Module は、デフォルトで 802.3 パケットをブリッジします。したがって、802.3 ブリッジをディセーブルにできるのは、4400 シリーズ コントローラ、Cisco WiSM、および Catalyst 3750G Wireless LAN コントローラ スイッチだけです。

802.3 ブリッジのステータスを決定するには、**show netuser guest-roles** コマンドを入力します。

次に、802.3 ブリッジを有効にする例を示します。

```
(Cisco Controller) > config network 802.3-bridging enable
```

関連コマンド

show netuser guest-roles

show network

config network allow-old-bridge-aps

スイッチとアソシエートする古いブリッジ アクセス ポイントの機能を設定するには、**config network allow-old-bridge-aps** コマンドを使用します。

config network allow-old-bridge-aps {**enable** | **disable**}

構文の説明

enable	スイッチ アソシエーションをイネーブルにします。
disable	スイッチ アソシエーションをディセーブルにします。

コマンド デフォルト

スイッチ アソシエーションは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、古いブリッジアクセスポイントをスイッチに関連付けるように設定する例を示します。

```
(Cisco Controller) > config network allow-old-bridge-aps enable
```

config network ap-discovery

AP ディスカバリ応答で NAT IP を有効または無効にするには、**config network ap-discovery** コマンドを使用します。

config network ap-discovery nat-ip-only {**enable** | **disable**}

構文の説明

enable	NAT IP の使用をディスカバリ応答でのみイネーブルにします。
disable	ディスカバリ応答での NAT IP および非 NAT IP の両方の使用をイネーブルにします。

コマンド デフォルト

NAT IP の使用がディスカバリ応答でのみ有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config interface nat-address management コマンドが設定されている場合、このコマンドによって、CAPWAP ディスカバリ応答で送信されるアドレスが制御されます。

すべての AP がコントローラの NAT ゲートウェイの外側にある場合、**config network ap-discovery nat-ip-only enable** コマンドを入力して、管理 NAT アドレスのみを送信します。

コントローラが、NAT ゲートウェイの外部と内部の両方に AP を持つ場合、**config network ap-discovery nat-ip-only disable** コマンドを入力して、管理 NAT アドレスと管理内部アドレスの両方を送信します。AP が取り残されないように、**config ap link-latency disable all** コマンドを必ず入力してください。

次に、AP ディスカバリ応答で NAT IP を有効にする例を示します。

```
(Cisco Controller) > config network ap-discovery nat-ip-only enable
```

config network ap-easyadmin

Cisco AP の EasyAdmin 機能を設定するには、**config network ap-easyadmin** コマンドを使用します。

config network ap-easyadmin {**enable** | **disable**}

構文の説明

enable	AP の EasyAdmin を有効にします。
disable	AP の EasyAdmin を無効にします。

コマンド デフォルト

EasyAdmin は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
8.4	このリリースでこのコマンドが追加されました。

次に、Cisco AP の EasyAdmin を有効にする例を示します。

```
(Cisco Controller) > config network ap-easyadmin enable
```

config network ap-fallback

Cisco Lightweight アクセス ポイントのフォールバックを設定するには、**config network ap-fallback** コマンドを使用します。

config network ap-fallback {**enable** | **disable**}

構文の説明

enable	Cisco Lightweight アクセス ポイントのフォール バックをイネーブルにします。
disable	Cisco Lightweight アクセス ポイントのフォール バックをディセーブルにします。

コマンド デフォルト

Cisco Lightweight アクセス ポイントのフォール バックは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco Lightweight アクセス ポイントのフォール バックを有効にする例を示します。

```
(Cisco Controller) > config network ap-fallback enable
```

config network ap-priority

Lightweight アクセス ポイントを優先するオプションを有効または無効にして、コントローラ障害後にコントローラが先着順ではなく優先順位によって再認証されるようにするには、**config network ap-priority** コマンドを使用します。

config network ap-priority {**enable** | **disable**}

構文の説明

enable	Lightweight アクセス ポイントの優先順位による再認証をイネーブルにします。
disable	Lightweight アクセス ポイントの優先順位による再認証をディセーブルにします。

コマンド デフォルト

Lightweight アクセス ポイントの優先順位による再認証は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Lightweight アクセス ポイントの優先順位による再認証を有効にする例を示します。

```
(Cisco Controller) > config network ap-priority enable
```

config network apple-talk

AppleTalk ブリッジを設定するには、**config network apple-talk** コマンドを使用します。

config network apple-talk {**enable** | **disable**}

構文の説明

enable	AppleTalk のブリッジをイネーブルにします。
disable	AppleTalk のブリッジをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、AppleTalk のブリッジを設定する例を示します。

```
(Cisco Controller) > config network apple-talk enable
```

config network arptimeout

Address Resolution Protocol（ARP）エントリのタイムアウト値を設定するには、**config network arptimeout** コマンドを使用します。

config network arptimeout *seconds*

構文の説明

seconds	秒単位のタイムアウト値です。最小値は10秒です。デフォルト値は 300 秒です。

コマンド デフォルト

デフォルトの ARP エントリ タイムアウト値は 300 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、ARP エントリのタイムアウト値を 240 秒に設定する例を示します。

```
(Cisco Controller) > config network arptimeout 240
```

関連コマンド

show network summary

config assisted-roaming

コントローラ上に経由ローミング パラメータを設定するには、**config assisted-roaming** コマンドを使用します。

config assisted-roaming {**denial-maximum** *count* | **floor-bias** *RSSI* | **prediction-minimum** *number_of_APs*}

構文の説明

denial-maximum	アソシエーション拒否の最大カウントを設定します。
count	アクセス ポイントに送信されたアソシエーション リクエストが予測リストのどのアクセス ポイントにも一致しない場合に、クライアントがアソシエーションに拒否される最大回数。値の範囲は 1 ～ 10 です。
floor-bias	同一フロア上のアクセス ポイントに RSSI バイアスを設定します。
RSSI	同一フロア上のアクセス ポイントに対する RSSI バイアス。範囲は 5 ～ 25 です。同一フロア上のアクセス ポイントにはより多くのプリファレンスがあります。
prediction-minimum	経由ローミング機能向けに最適化されたアクセス ポイントの最小数を設定します。
number_of_APs	経由ローミング機能向けに最適化されたアクセス ポイントの最小数。指定できる範囲は1～6です。クライアントに割り当てられた予測のアクセス ポイント数がこの値より小さい場合、経由ローミングは機能しません。

コマンド デフォルト

同一フロア上のアクセス ポイントのデフォルト RSSI バイアスは 15 dBm です。

使用上のガイドライン

802.11k では、クライアントはサービス セットの遷移に使用できる、既知のネイバー アクセス ポイントに関する情報を含むネイバー レポートを要求できるようになります。ネイバー リストによって、アクティブ スキャンおよびパッシブ スキャンを行う必要性が低減されます。

次に、経由ローミング機能向けに最適化されたアクセス ポイントの最小数を設定する例を示します。

```
(Cisco Controller) >config assisted-roaming prediction-minimum 4
```

config network bridging-shared-secret

ブリッジの共有キーを設定するには、**config network bridging-shared-secret** コマンドを使用します。

config network bridging-shared-secret *shared_secret*

構文の説明

shared_secret	ブリッジの共有キーの文字列。文字列には 10 バイトまで使用できます。

コマンド デフォルト

ブリッジの共有キーは、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドにより、スイッチに接続するメッシュ アクセス ポイントのバックホール ユーザ データを暗号化する共有キーが作成されます。

このコマンドを機能させるには、zero touch configuration をイネーブルにしておく必要があります。

次に、ブリッジの共有キーの文字列「shhh1」を設定する例を示します。

```
(Cisco Controller) > config network bridging-shared-secret shhh1
```

関連コマンド

show network summary

config network broadcast

ブロードキャスト パケット転送を有効または無効にするには、**config network broadcast** コマンドを使用します。

config network broadcast {**enable** | **disable**}

構文の説明

enable	ブロードキャスト パケットの転送をイネーブルにします。
disable	ブロードキャスト パケットの転送をディセーブルにします。

コマンド デフォルト

ブロードキャスト パケットの転送は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用すると、ブロードキャストをイネーブルまたはディセーブルにすることができます。ブロードキャスト転送をイネーブルにする前に、マルチキャスト モードをイネーブルにする必要があります。**config network multicast mode command** コマンドを使用して、コントローラにマルチキャスト モードを設定します。

（注） デフォルトのマルチキャスト モードは、Cisco 2106 コントローラを除くすべてのコントローラの場合はユニキャストです。ブロードキャスト パケットおよびマルチキャスト パケットは個別に制御できます。マルチキャストがオフになり、ブロードキャストがオンになっても、ブロードキャスト パケットは設定されたマルチキャスト モードに基づいてアクセス ポイントに到達します。

次に、ブロードキャスト パケットの転送を有効にする例を示します。

```
(Cisco Controller) > config network broadcast enable
```

関連コマンド

show network summary

config network multicast global

config network multicast mode

config network fast-ssid-change

モバイル端末で高速サービス セット ID（SSID）の変更を有効または無効にするには、**config network fast-ssid-change** コマンドを使用します。

config network fast-ssid-change {**enable** | **disable**}

構文の説明

enable	モバイル ステーションに対して、高速 SSID の変更をイネーブルにします
disable	モバイル ステーションに対して、高速 SSID の変更をディセーブルにします

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

高速 SSID 変更機能を有効にすると、クライアントは SSID 間を移動できます。クライアントが異なる SSID の新しいアソシエーションを送信すると、コントローラの通信テーブルのクライアント エントリがクリアされてから、新しい SSID にクライアントが追加されます。

高速 SSID 変更機能を無効にすると、コントローラによる強制遅延後にクライアントが新しい SSID に移動できます。

次に、モバイル ステーションに対して、高速 SSID の変更を有効にする例を示します。

```
(Cisco Controller) > config network fast-ssid-change enable
```

関連コマンド

show network summary

config network ip-mac-binding

クライアント パケット内での送信元 IP アドレスと MAC アドレスのバインディングを検証するには、**config network ip-mac-binding** コマンドを使用します。

config network ip-network-binding {**enable** | **disable**}

構文の説明

enable	クライアント パケット内での送信元 IP アドレスの MAC アドレスへのバインディングの検証を有効にします。
disable	クライアント パケット内での送信元 IP アドレスの MAC アドレスへのバインディングの検証を無効にします。

コマンド デフォルト

クライアント パケット内での送信元 IP アドレスの MAC アドレスへのバインディングの検証は、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラ ソフトウェア リリース 5.2 では、コントローラがクライアント パケット内の IP アドレスと MAC アドレスとの厳密なバインディングを行います。コントローラは、パケット内の IP アドレスおよび MAC アドレスを確認し、これらのアドレスとコントローラに登録されているアドレスを比較します。パケットは、両方が一致した場合に限り転送されます。以前のリリースでは、クライアントの MAC アドレスだけが確認され、IP アドレスは無視されていました。

（注） Workgroup Bridge（WGB）の背後にルーテッド ネットワークが存在する場合は、このバインディング チェックを無効にすることを推奨します。

次に、クライアント パケット内の送信元 IP アドレスと MAC アドレスを検証する例を示します。

```
(Cisco Controller) > config network ip-mac-binding enable
```

config network link local bridging

ローカルサイトでリンク ローカル トラフィックのブリッジングを設定するには、**config network link-local-bridging** コマンドを使用します。

config network link-local-bridging {**enable** | **disable**}

構文の説明

enable	ローカルサイトでリンク ローカル トラフィックのブリッジングを有効にします。
disable	ローカルサイトでリンク ローカル トラフィックのブリッジングを無効にします。

コマンド デフォルト

無効

コマンド履歴

リリース	変更内容
8.0	このコマンドが追加されました。

config network master-base

Cisco ワイヤレス LAN コントローラをアクセス ポイントのデフォルト マスターとして有効または無効にするには、**config network master-base** コマンドを使用します。

config network master-base {**enable** | **disable**}

構文の説明

enable	Cisco Lightweight アクセス ポイントのデフォルト マスターとして機能している Cisco ワイヤレス LAN コントローラをイネーブルにします。
disable	Cisco Lightweight アクセス ポイントのデフォルト マスターとして機能している Cisco ワイヤレス LAN コントローラをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

この設定はネットワークのインストール時にのみ使用され、初期ネットワーク設定後は無効にする必要があります。通常、マスター Cisco ワイヤレス LAN コントローラは展開済みネットワークでは使用されないため、マスター Cisco ワイヤレス LAN コントローラの設定は 6.0.199.0 以降のリリースから保存できます。

次に、デフォルト マスターとして Cisco ワイヤレス LAN コントローラを有効にする例を示します。

```
(Cisco Controller) > config network master-base enable
```

config network mgmt-via-wireless

関連付けられている無線クライアントから Cisco ワイヤレス LAN コントローラを管理できるようにするには、**config network mgmt-via-wireless** コマンドを使用します。

config network mgmt-via-wireless {**enable** | **disable**}

構文の説明

enable	ワイヤレス インターフェイスからスイッチ管理をイネーブルにします。
disable	ワイヤレス インターフェイスからスイッチ管理をディセーブルにします。

コマンド デフォルト

ワイヤレス インターフェイスからのスイッチ管理は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

この機能を使用して無線クライアントが管理できるのは、そのクライアントに関連付けられた Cisco ワイヤレス LAN コントローラと、関連付けられた Cisco Lightweight アクセス ポイントのみです。つまり、関連付けられていない他の Cisco ワイヤレス LAN コントローラは管理できません。

次に、ワイヤレス インターフェイスからスイッチ管理を設定する例を示します。

```
(Cisco Controller) > config network mgmt-via-wireless enable
```

関連コマンド

show network summary

config network multicast global

コントローラでマルチキャストを有効または無効にするには、**config network multicast global** コマンドを使用します。

config network multicast global {**enable** | **disable**}

構文の説明

enable	マルチキャスト グローバル サポートをイネーブルにします。
disable	マルチキャスト グローバル サポートをディセーブルにします。

コマンド デフォルト

コントローラでのマルチキャストは、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config network broadcast {**enable** | **disable**} コマンドを使用すると、マルチキャスティングを有効または無効にすることなく、ブロードキャスティングを有効または無効にすることができます。このコマンドは、（**config network multicast mode command)** コマンド）を使用して操作するコントローラに設定されたマルチキャスト モードを使用します。

次に、グローバルなマルチキャスト サポートを有効にする例を示します。

```
(Cisco Controller) > config network multicast global enable
```

関連コマンド

show network summary

config network broadcast

config network multicast mode

config network multicast igmp query interval

IGMP クエリー間隔を設定するには、**config network multicast igmp query interval** コマンドを使用します。

config network multicast igmp query interval *value*

構文の説明

value	コントローラが IGMP クエリー メッセージを送信する頻度。範囲は 15 ～ 2400 秒です。

コマンド デフォルト

デフォルトの IGMP クエリー間隔は 20 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

IGMP クエリー間隔を設定するには、次の手順を実行します。

- **config network multicast global enable** コマンドを入力して、グローバル マルチキャストを有効にします。
- **config network multicast igmp snooping enable** コマンドを入力して、IGMP スヌーピングを有効にします。

次に、IGMP クエリー間隔を設定 20 秒に設定する例を示します。

```
(Cisco Controller) > config network multicast igmp query interval 20
```

関連コマンド

config network multicast global

config network multicast igmp snooping

config network multicast igmp timeout

config network multicast igmp snooping

IGMP スヌーピングを有効または無効にするには、**config network multicast igmp snooping** コマンドを使用します。

config network multicast igmp snooping {**enable** | **disable**}

構文の説明

enable	IGMP スヌーピングをイネーブルにします。
disable	IGMP スヌーピングをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、インターネットの IGMP スヌーピング設定を有効にする例を示します。

```
(Cisco Controller) > config network multicast igmp snooping enable
```

関連コマンド

config network multicast global

config network multicast igmp query interval

config network multicast igmp timeout

config network multicast igmp timeout

IGMP タイムアウト値を設定するには、**config network multicast igmp timeout** コマンドを使用します。

config network multicast igmp timeout *value*

構文の説明

value	30 ～ 7200 秒のタイムアウトの範囲。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

timeout には、30 ～ 7200 秒の値を入力できます。特定のマルチキャスト グループに対してクライアントが存在するかどうかを確認するために、コントローラから、1 つのタイムアウト値につき 3 つのクエリが timeout/3 の間隔で送信されます。クライアントから、IGMP レポートを通じて応答を受け取らなかった場合、コントローラはこのクライアントのエントリを MGID テーブルからタイムアウトします。特定のマルチキャスト グループに対するクライアントが残されていない場合、クライアントは IGMP タイムアウト値が経過するまで待ってから、コントローラから MGID エントリを削除します。このコントローラは（宛先アドレス 224.0.0.1 に対して）常に一般的な IGMP クエリーを生成し、MGID 値が 1 である WLAN すべてに送信します。

次に、IGMP ネットワーク設定のタイムアウト値 50 を設定する例を示します。

```
(Cisco Controller) > config network multicast igmp timeout 50
```

関連コマンド

config network multicast global

config network igmp snooping

config network multicast igmp query interval

config network multicast l2mcast

1 つのインターフェイスまたはすべてのインターフェイスにレイヤ 2 マルチキャストを設定するには、**config network multicast l2mcast** コマンドを使用します。

config network multicast l2mcast {**enable** | **disable** {**all** | *interface-name*}

構文の説明

enable	レイヤ 2 マルチキャストをイネーブルにします。
disable	レイヤ 2 マルチキャストをディセーブルにします。
all	すべてのインターフェイスに適用します。
interface-name	レイヤ 2 マルチキャストがイネーブルまたはディセーブルにされたインターフェイス名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのインターフェイスに対してレイヤ 2 マルチキャストを有効にする例を示します。

```
(Cisco Controller) > config network multicast l2mcast enable all
```

関連コマンド

config network multicast global

config network multicast igmp snooping

config network multicast igmp query interval

config network multicast mld

config network multicast mld

Multicast Listener Discovery（MLD）パラメータを設定するには、**config network multicast mld** コマンドを使用します。

config network multicast mld {**query interval** *interval-value* | **snooping** {**enable** | **disable**} | **timeout** *timeout-value*}

構文の説明

query interval	MLD クエリー メッセージを送信するようにクエリー間隔を設定します。
interval-value	秒単位のクエリー間隔です。範囲は 15 ～ 2400 秒です。
snooping	MLD スヌーピングを設定します。
enable	MLD スヌーピングをイネーブルにします。
disable	MLD スヌーピングをディセーブルにします。
timeout	MLD のタイムアウトを設定します。
timeout-value	秒単位のタイムアウト値です。範囲は 30 ～ 7200 秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MLD クエリー メッセージに 20 秒のクエリー間隔を設定する例を示します。

```
(Cisco Controller) > config network multicast mld query interval 20
```

関連コマンド

config network multicast global

config network multicast igmp snooping

config network multicast igmp query interval

config network multicast l2mcast

config network multicast mode multicast

ブロードキャストパケットまたはマルチキャストパケットをアクセスポイントに送信する際、マルチキャスト方式を使用するようにコントローラを設定するには、**config network multicast mode multicast** コマンドを使用します。

config network multicast mode multicast

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、マルチキャスト レシーバにデータのコピーを 1 つ送信するマルチキャスト モードを設定する例を示します。

```
(Cisco Controller) > config network multicast mode multicast
```

関連コマンド

config network multicast global

config network broadcast

config network multicast mode unicast

config network multicast mode unicast

ブロードキャストパケットまたはマルチキャストパケットをアクセスポイントに送信する際、ユニキャスト方式を使用するようにコントローラを設定するには、**config network multicast mode unicast** コマンドを使用します。

config network multicast mode unicast

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コントローラがユニキャスト モードを使用するように設定する例を示します。

```
(Cisco Controller) > config network multicast mode unicast
```

関連コマンド

config network multicast global

config network broadcast

config network multicast mode multicast

config network oeap-600 dual-rlan-ports

Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、ポート 4 に加えて、リモート LAN ポートとしても機能するように設定するには、**config network oeap-600 dual-rlan-ports** コマンドを使用します。

config network oeap-600 dual-rlan-ports {**enable** | **disable**}

構文の説明

enable	Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、ポート 4 に加えて、リモート LAN ポートとしても機能できるようにします。
disable	Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネットポート3をリセットして、ローカル LAN ポートとして機能するようにします。

コマンド デフォルト

Cisco 600 シリーズ OEAP のイーサネット ポート 3 がリセットされます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、リモートの LAN ポートとして機能できるようにする例を示します。

```
(Cisco Controller) > config network oeap-600 dual-rlan-ports enable
```

config network oeap-600 local-network

Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスを設定するには、**config network oeap-600 local-network** コマンドを使用します。

config network oeap-600 local-network {**enable** | **disable**}

構文の説明

enable	Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスをイネーブルにします。
disable	Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスをディセーブルにします。

コマンド デフォルト

Cisco 600 シリーズ OEAP のローカル ネットワークへのアクセスは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスを有効にする例を示します。

```
(Cisco Controller) > config network oeap-600 local-network enable
```

config network otap-mode

Cisco Lightweight アクセス ポイントの無線プロビジョニング（OTAP）を有効または無効にするには、**config network otap-mode** コマンドを使用します。

config network otap-mode {**enable** | **disable**}

構文の説明

enable	OTAP プロビジョニングをイネーブルにします。
disable	OTAP プロビジョニングをディセーブルにします。

コマンド デフォルト

OTAP プロビジョニングは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、OTAP プロビジョニングを無効にする例を示します。

```
(Cisco Controller) >config network otap-mode disable
```

config network profiling

特定のポートの HTTP ポートをプロファイルするには、**config network profiling http-port** コマンドを使用します。

config network profiling http-port ポート番号

構文の説明

ポート番号	インターフェイス ポート番号。デフォルト値は 80 です。

コマンド履歴

リリース	変更内容
8.2	このコマンドが追加されました。

次に、ネットワークの HTTP ポートを設定する例を示します。

```
(Cisco Controller) > config network profiling http-port 80
```

config opendns

シスコ ワイヤレス コントローラ（WLC）でオープン ドメイン ネーム システム（DNS）を有効または無効にするには、**config opendns** コマンドを使用します。

config opendns { **enable** | **disable** }

構文の説明

enable	Opendns グローバル設定を有効にします。
disable	Opendns グローバル設定を無効にします。

コマンド デフォルト

オープン DNS は設定されていません。

コマンド モード

Controller Config >

コマンド履歴

リリース	変更内容
8.4	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、Cisco WLC でオープン DNS を有効にする例を示します。

```
(Cisco Controller) > config opendns enable
```

config opendns api-token

シスコ ワイヤレス コントローラ（WLC）に登録するための OpenDNS API トークン ヘルプを有効または無効にするには、**config opendns api-token** コマンドを使用します。

config opendns api-token *api-token*

構文の説明

api-token	OpenDNS の API トークン。

コマンド モード

（コントローラの設定）>

コマンド履歴

リリース	変更内容
8.4	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、Cisco WLC で OpenDNS を登録するための API トークン ヘルプを有効にする例を示します。

```
(Cisco Controller) > config opendns api-token 12
```

config opendns forced

シスコ ワイヤレス コントローラ（WLC）で OpenDNS を有効または無効にするには、**config opendns forced** コマンドを使用します。

config opendns forced {**enable** | **disable**}

構文の説明

enable	OpenDNS グローバル設定を有効にします。
disable	OpenDNS グローバル設定を無効にします。

コマンド デフォルト

OpenDNS は設定されていません。

コマンド モード

（コントローラの設定）>

コマンド履歴

リリース	変更内容
8.4	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、Cisco WLC で OpenDNS を有効にする例を示します。

```
(Cisco Controller) > config opendns forced enable
```

config opendns profile

ユーザ グループ、ワイヤレス LAN（WLAN）、またはサイトに適用できる OpenDNS のプロファイルを設定するには、**config opendns profile** コマンドを使用します。

config opendns profile{ **create** | **delete** | **refresh**} *profile-name*

構文の説明

create	OpenDNS アイデンティティ名を作成します。
delete	OpenDNS アイデンティティ名を削除します。
refresh	現在の状態に関係なく、登録を再トリガして OpenDNS アイデンティティを更新します。
profile-name	OpenDNS アイデンティティの名前。

コマンド デフォルト

OpenDNS プロファイルは作成されません。

コマンド モード

（コントローラの設定）>

コマンド履歴

リリース	変更内容
8.4	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、ユーザ グループに適用できる OpenDNS のプロファイルを設定する例を示します。

```
(Cisco Controller) > config opendns profile create usergroup1
```

config pmipv6 domain

PMIPv6 を設定し、Cisco のモバイル アクセス ゲートウェイ（MAG）機能を有効にするには、**config pmipv6 domain** コマンドを使用します。

config pmipv6 domain *domain_name*

構文の説明

domain_name	PMIPv6 ドメインの名前。ドメイン名は最大 127 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、PMIPv6 WLAN のドメイン名を設定する例を示します。

```
(Cisco Controller) >config pmipv6 domain floor1
```

config pmipv6 add profile

WLAN のプロキシ モビリティ IPv6（PMIPv6）プロファイルを作成するには、**config pmipv6 add profile** コマンドを使用します。レルムまたは Service Set Identifier（SSID）に基づいて、PMIPv6 プロファイルを設定できます。

config pmipv6 add profile *profile_name* **nai** {*user@realm* | *@realm* | *****} **lma** *lma_name* **apn** *apn_name*

構文の説明

profile_name	プロファイルの名前プロファイル名は最大 127 文字の英数字で、大文字と小文字を区別します。
nai	クライアントのネットワーク アクセス ID を指定します。
user@realm	*user*@realm 形式のクライアントのネットワーク アクセス ID。NAI 名は最大 127 文字の英数字で、大文字と小文字を区別します。
@realm	@realm 形式のクライアントのネットワーク アクセス ID。
*	すべてのネットワーク アクセス ID。すべてのユーザに対して、SSID に基づいてプロファイルを用意できます。
lma	Local Mobility Anchor（LMA）を指定します。
lma_name	LMA の名前。LMA 名は最大 127 文字の英数字で、大文字と小文字を区別します。
apn	アクセス ポイントを指定します。
ap_name	アクセス ポイントの名前。アクセス ポイント名は最大 127 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラがオープン認証を使用する場合、このコマンドは、PMIPv6 コンフィギュレーション コマンドを使用するための前提条件です。

次に、PMIPv6 プロファイルを作成する例を示します。

```
(Cisco Controller) >config pmipv6 add profile profile1 nai @vodfone.com lma vodfonelma
apn vodafoneapn
```

config pmipv6 delete

プロキシ モビリティ IPv6（PMIPv6）プロファイル、ドメイン、または Local Mobility Anchor（LMA）を削除するには、 **config pmipv6 delete** コマンドを使用します。

config pmipv6 delete {**profile** *profile_name* **nai** { *nai_id* | **all** } | **domain** *domain_name* | **lma** *lma_name*}

構文の説明

profile	PMIPv6 プロファイルを指定します。
profile_name	PMIPv6 プロファイルの名前。プロファイル名は最大 127 文字の英数字で、大文字と小文字を区別します。
nai	モバイル クライアントのネットワーク アクセス ID（NAI）を指定します。
nai_id	モバイル クライアントのネットワーク アクセス ID。NAI は最大 127 文字の英数字で、大文字と小文字を区別します。
all	すべての NAI を指定します。すべての NAI を削除すると、プロファイルが削除されます。
domain	PMIPv6 ドメインを指定します。
domain_name	PMIPv6 ドメインの名前。ドメイン名は最大 127 文字の英数字で、大文字と小文字を区別します。
lma	LMA を指定します。
lma_name	LMA の名前。LMA 名は最大 127 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ドメインを削除する例を示します。

```
(Cisco Controller) >config pmipv6 delete lab1
```

config pmipv6 mag apn

モバイル アクセス ゲートウェイ（MAG）のアクセス ポイント名（APN）を設定するには、**config pmipv6 mag apn** コマンドを使用します。

config pmipv6 mag apn *apn-name*

構文の説明

apn-name	MAGのアクセスポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、MAG ロールは WLAN です。ただし Lightweight アクセス ポイントの場合、MAG ロールは 3GPP に設定する必要があります。MAG ロールが 3GPP の場合、MAG の APN を指定する必要があります。

MAG の APN を削除するには、**config pmipv6 delete mag apn** *apn-name* コマンドを使用します。

次に、MAG の APN を追加する例を示します。

```
(Cisco Controller) >config pmipv6 mag apn myCiscoAP
```

config pmipv6 mag binding init-retx-time

モバイルアクセス ゲートウェイ（MAG）がプロキシ バインディング確認（PBA）を受信しない場合のプロキシ バインディング アップデート（PBU）間の初期タイムアウトを設定するには、 **config pmipv6 mag binding init-retx-time** コマンドを使用します。

config pmipv6 mag binding init-retx-time *units*

構文の説明

units	MAG が PBA を受信しない場合の PBU 間の初期タイムアウト。範囲は 100 ～ 65535 秒です。

コマンド デフォルト

デフォルトの初期タイムアウトは 1000 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAG が PBA を受信しない場合に PBU 間の初期タイムアウトを設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag binding init-retx-time 500
```

config pmipv6 mag binding lifetime

モバイルアクセス ゲートウェイ（MAG）のバインディングエントリのライフタイムを設定するには、 **config pmipv6 mag binding lifetime** コマンドを使用します。

config pmipv6 mag binding lifetime *units*

構文の説明

units	MAG のバインディング エントリのライフタイム。バインディング ライフタイムは 4 秒の倍数であることが必要です。範囲は 10 ～ 65535 秒です。

コマンド デフォルト

バインディング エントリのデフォルトのライフタイムは 65535 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラのバインディングエントリのライフタイムを設定する前に、プロキシモビリティ IPv6（PMIPv6）ドメインを設定する必要があります。

次に、コントローラのバインディングエントリのライフタイムを設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag binding lifetime 5000
```

config pmipv6 mag binding max-retx-time

モビリティ アクセス ゲートウェイ（MAG）がプロキシ バインディング確認（PBA）を受信しない場合のプロキシ バインディング アップデート（PBU）間の最大タイムアウトを設定するには、 **config pmipv6 mag binding max-retx-time** コマンドを使用します。

config pmipv6 mag binding max-retx-time *units*

構文の説明

units	MAG が PBA を受信しない場合の PBU 間の最大タイムアウト。範囲は 100 ～ 65535 秒です。

コマンド デフォルト

デフォルトの最大タイムアウトは 32000 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAG が PBA を受信しない場合の PBU 間の最大タイムアウトを設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag binding max-retx-time 50
```

config pmipv6 mag binding maximum

モバイル アクセス ゲートウェイ（MAG）のバインディング エントリの最大数を設定するには、 **config pmipv6 mag binding maximum** コマンドを使用します。

config pmipv6 mag binding maximum *units*

構文の説明

units	MAG のバインディング エントリの最大数。この番号は、MAG に接続されるユーザの最大数を示します。範囲は 0 ～ 40000 です。

コマンド デフォルト

MAG のバインディング エントリのデフォルトの最大数は 10000 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

MAG のバインディング エントリの最大数を設定する前に、プロキシモビリティ IPv6（PMIPv6）ドメインを設定する必要があります。

次に、MAG のバインディング エントリの最大数を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag binding maximum 20000
```

config pmipv6 mag binding refresh-time

MAG のバインディング エントリのリフレッシュ時間を設定するには、 **config pmipv6 mag binding refresh-time** コマンドを使用します。

config pmipv6 mag binding refresh-time *units*

構文の説明

units	MAGのバインディングエントリのリフレッシュ時間。バインディングのリフレッシュ時間は、4 の倍数である必要があります。範囲は 4 ～ 65535 秒です。

コマンド デフォルト

MAG のバインディング エントリのリフレッシュ時間は、デフォルトでは 300 秒です。

使用上のガイドライン

MAG のバインディング エントリのリフレッシュ時間を設定する前に、PMIPv6 ドメインを設定する必要があります。

次に、MAGのバインディングエントリのリフレッシュ時間を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag binding refresh-time 500
```

config pmipv6 mag bri delay

MAG が Binding Revocation Indication（BRI）メッセージを再送信するまでに待機する最大時間または最小時間を設定するには、 **config pmipv6 mag bri delay** コマンドを使用します。

config pmipv6 mag bri delay {**min** | **max**} *time*

構文の説明

min	MAG が BRI メッセージを再送信するまでに待機する最小時間を指定します。
max	MAG が BRI メッセージを再送信するまでに待機する最大時間を指定します。
time	Cisco WLC が BRI メッセージを再送信するまでに待機する最大時間または最小時間。指定できる範囲は 500 ～ 65535 ミリ秒です。

コマンド デフォルト

MAG が BRI メッセージを再送信するまでに待機する最大時間のデフォルト値は 2 秒です。

MAG が BRI メッセージを再送信するまでに待機する最小時間のデフォルト値は 1 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAG が BRI メッセージを再送信するまでに待機する最大時間を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag bri delay min 500
```

config pmipv6 mag bri retries

MAG が Binding Revocation Acknowledgement（BRA）メッセージを受信する前に Binding Revocation Indication（BRI）メッセージを再送信する最大回数を設定するには、**config pmipv6 mag bri retries** コマンドを使用します。

config pmipv6 mag bri retries *retries*

構文の説明

retries	MAG が BRA メッセージを受信する前に BRI メッセージを再送信する最大回数。指定できる範囲は 1 ー 10 回です。

コマンド デフォルト

デフォルトは 1 回です。

次に、MAG が再試行する最大回数を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag bri retries 5
```

config pmipv6 mag lma

モバイル アクセス ゲートウェイ（MAG）でローカル モビリティ アンカー（LMA）を設定するには、 **config pmipv6 mag lma** コマンドを使用します。

config pmipv6 mag lma *lma_name* **ipv4-address** *address*

構文の説明

lma_name	LMA の名前。LMA 名は、LMA を一意に識別する NAI または文字列にすることができます。
ipv4-address	LMA の IP アドレスを指定します。
address	LMA の IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、MAG で PMIPv6 のパラメータを設定するための前提条件です。

次に、MAG で LMA を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag lma vodafonelma ipv4-address 209.165.200.254
```

config pmipv6 mag replay-protection

リプレイ保護のために、受信したプロキシバインディング確認（PBA）のタイムスタンプと現在の日時との最大時間差を設定するには、 **config pmipv6 mag replay-protection** コマンドを使用します。

config pmipv6 mag replay-protection { **timestamp window** *time* | **sequence-no** *sequence* | **mobile-node-timestamp** *mobile_node_timestamp* }

構文の説明

timestamp	PBA メッセージのタイムスタンプを指定します。
window	受信した PBA メッセージのタイムスタンプと現在時刻間の最大時間差を指定します。
time	受信した PBA メッセージのタイムスタンプと現在時刻間の最大時間差。範囲は 1 ～ 300 ミリ秒です。
sequence-no	（任意）Proxy Binding Update メッセージのシーケンス番号を指定します。
sequence	（任意）Proxy Binding Update メッセージのシーケンス番号。
mobile_node_timestamp	（任意）モバイルノードのタイムスタンプを指定します。
mobile_node_timestamp	（任意）モバイル ノードのタイムスタンプ。

コマンド デフォルト

デフォルトの最大時間差は 300 ミリ秒です。

使用上のガイドライン

タイムスタンプ オプションだけがサポートされています。

次に、受信したPBAメッセージのタイムスタンプと現在時刻間の最大時間差（ミリ秒単位）を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag replay-protection timestamp window 200
```

config port power

特定のコントローラ ポートまたはすべてのポートの Power over Ethernet（PoE）を有効または無効にするには、**config port power** コマンドを使用します。

config port power {**all** | *port*} {**enable** | **disable**}

構文の説明

all	すべてのポートを設定します。
port	ポート番号。
enable	指定したポートをイネーブルにします。
disable	指定したポートをディセーブルにします。

コマンド デフォルト

イネーブル

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのポートで PoE を有効にする例を示します。

```
(Cisco Controller) > config port power all enable
```

次に、ポート 8 で PoE を無効にする例を示します。

```
(Cisco Controller) > config port power 8 disable
```

config policy action opendns-profile-name

ポリシーに対してOpenDNSアクションを設定するには、**config policy action opendns-profile-name** コマンドを使用します。

config policy *policy-name* **action opendns-profile-name**{**enable** | **disable**}

構文の説明

policy-name	ポリシー名（iPad、iPhone、smartphoneなど）。
enable	アクションを有効にします。
disable	アクションを無効にします。

コマンド モード

（コントローラの設定）>

コマンド履歴

リリース	変更内容
8.4	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、ポリシーに対して OpenDNS アクションを設定する例を示します。

```
(Cisco Controller) > config policy ipad action opendns-profile-name enable
```

config network rf-network-name

RF ネットワーク名を設定するには、**config network rf-network-name** コマンドを使用します。

config network rf-network-name *name*

構文の説明

name	RF ネットワーク名。名前には最大 19 文字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、旅行者に RF ネットワーク名を設定する例を示します。

```
(Cisco Controller) > config network rf-network-name travelers
```

関連コマンド

show network summary

config network secureweb

管理ユーザのセキュア Web（https は http および SSL）インターフェイスの状態を変更するには、**config network secureweb** コマンドを使用します。

config network secureweb {**enable** | **disable**}

構文の説明

enable	管理ユーザのセキュア Web インターフェイスをイネーブルにします。
disable	管理ユーザのセキュア Web インターフェイスをディセーブルにします。

コマンド デフォルト

管理ユーザのセキュア Web インターフェイスは、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドにより、管理ユーザは http://ip-address を使用してコントローラの GUI にアクセスできるようになります。Web モードの接続は、セキュリティで保護されません。

次に、管理ユーザのセキュア Web インターフェイス設定を有効にする例を示します。

```
(Cisco Controller) > config network secureweb enable
You must reboot for the change to take effect.
```

関連コマンド

config network secureweb cipher-option

show network summary

config network secureweb cipher-option

セキュリティを強化したセキュアWebモードを有効または無効にするか、Web管理およびWeb認証用のセキュア ソケット レイヤ（SSL v2）を有効または無効にするには、**config network secureweb cipher-option** コマンドを使用します。

config network secureweb cipher-option {**high** | **sslv2** | **rc4-preference**} {**enable** | **disable**}

構文の説明

high	Web 管理および Web 認証に 128 ビット暗号化が必要であるかどうかを設定します。
sslv2	Web 管理と Web 認証の両方に対して SSLv2 を設定します。
rc4-preference	Web 管理と Web 認証に関して、RC4-SHA（Rivest Cipher 4 セキュア ハッシュ アルゴリズム）暗号スイートを優先するように設定します。
enable	セキュア Web インターフェイスをイネーブルにします。
disable	セキュア Web インターフェイスをディセーブルにします。

コマンド デフォルト

セキュリティが強化されたセキュア Web モードの場合はデフォルトで **disable** であり、SSL v2 の場合は **enable** です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

（注） **config network secureweb cipher-option** コマンドを使用すると、http://ip-address を使用してコントローラ GUI にアクセスできるようになります。ただし、このアクセスは 128 ビット以上の暗号方式をサポートしているブラウザからに限り可能です。

cipher-option sslv2 が無効の場合、SSLv2 だけで設定されているブラウザを使用して接続することはできません。SSLv3 以降などセキュリティの強化されたプロトコルを使用するように設定されたブラウザを使用する必要があります。

RC4-SHA ベースの暗号スイートでは、RC4 が暗号化に使用され、SHA はメッセージ認証に使用されます。

次に、セキュリティが強化されたセキュア Web モードを有効にする例を示します。

```
(Cisco Controller) > config network secureweb cipher-option
```

次に、SSL V2 を無効にする例を示します。

```
(Cisco Controller) > config network secureweb cipher-option sslv2 disable
```

関連コマンド

config network secureweb

show network summary

config network ssh

新規セキュア シェル（SSH）セッションを有効または無効にするには、**config network ssh** コマンドを使用します。

config network ssh {**enable** | **disable**}

構文の説明

enable	新規 SSH セッションを許可します。
disable	新規 SSH セッションを拒否します。

コマンド デフォルト

新しい SSH セッションのデフォルト値は **disable** です。

次に、新規 SSH セッションを有効にする例を示します。

```
(Cisco Controller) > config network ssh enable
```

関連コマンド

show network summary

config network telnet

新規 Telnet セッションを許可または拒否するには、**config network telnet** コマンドを使用します

config network telnet {**enable** | **disable**}

構文の説明

enable	新規 Telnet セッションを許可します。
disable	新規 Telnet セッションを拒否します。

コマンド デフォルト

デフォルトでは、新規 Telnet セッションは拒否され、値は **disable** です。

使用上のガイドライン

Telnet は、Cisco Aironet 1830 および 1850 シリーズ アクセス ポイントではサポートされていません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、新規 Telnet セッションを設定する例を示します。

```
(Cisco Controller) > config network telnet enable
```

関連コマンド

config ap telnet

show network summary

config network usertimeout

アイドル状態のクライアント セッションのタイムアウトを変更するには、**config network usertimeout** コマンドを使用します。

config network usertimeout *seconds*

構文の説明

seconds	タイムアウト時間（秒）。最小値は 90 秒です。デフォルト値は 300 秒です。

コマンド デフォルト

アイドル状態のクライアント セッションのデフォルト タイムアウト値は 300 秒です。

使用上のガイドライン

このコマンドを使用して、Cisco ワイヤレス LAN コントローラ上のアイドル状態のクライアント セッション時間を設定します。最小時間は 90 秒です。

次に、アイドル セッション タイムアウトを 1200 秒に設定する例を示します。

```
(Cisco Controller) > config network usertimeout 1200
```

関連コマンド

show network summary

config network web-auth captive-bypass

ネットワーク レベルでキャプティブ ポータルのバイパスをサポートするようにコントローラを設定するには、**config network web-auth captive-bypass** コマンドを使用します。

config network web-auth captive-bypass {**enable** | **disable**}

構文の説明

enable	コントローラがキャプティブ ポータルのバイパスをサポートできるようにします。
disable	コントローラがキャプティブ ポータルのバイパスをサポートできないようにします。

コマンド デフォルト

なし

次に、キャプティブ ポータルのバイパスをサポートするようにコントローラを設定する例を示します。

```
(Cisco Controller) > config network web-auth captive-bypass enable
```

関連コマンド

show network summary

config network web-auth cmcc-support

config network web-auth cmcc-support

コントローラで eWalk を設定するには、**config network web-auth cmcc-support** コマンドを使用します。

config network web-auth cmcc-support {**enable** | **disable**}

構文の説明

enable	コントローラの eWalk をイネーブルにします。
disable	コントローラの eWalk をディセーブルにします。

コマンド デフォルト

なし

次に、コントローラの eWalk を有効にする例を示します。

```
(Cisco Controller) > config network web-auth cmcc-support enable
```

関連コマンド

show network summary

config network web-auth captive-bypass

config network web-auth port

ネットワーク レベルの Web 認証に関して追加ポートがリダイレクトされるように設定するには、**config network web-auth port** コマンドを使用します。

config network web-auth port *port*

構文の説明

port	ポート番号。有効な範囲は 0 ～ 65535 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web 認証に関して、追加ポート番号 1200 がリダイレクトされるように設定する例を示します。

```
(Cisco Controller) > config network web-auth port 1200
```

関連コマンド

show network summary

config network web-auth proxy-redirect

Web認証クライアントのプロキシのリダイレクションサポートを設定するには、**config network web-auth proxy-redirect** コマンドを使用します。

config network web-auth proxy-redirect {**enable** | **disable**}

構文の説明

enable	Web 認証クライアントのプロキシ リダイレクションをサポートできるようにします。
disable	Web 認証クライアントのプロキシ リダイレクションをサポートできないようにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、Web 認証クライアントのプロキシのリダイレクションのサポートを有効にする例を示します。

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

関連コマンド

show network summary

config network web-auth secureweb

クライアントにセキュア Web（https）認証を設定するには、**config network web-auth secureweb** コマンドを使用します。

config network web-auth secureweb {**enable** | **disable**}

構文の説明

enable	クライアントにセキュア Web（https）認証を行えるようにします。
disable	クライアントにセキュア Web（https）認証を行えないようにします。クライアントの HTTP Web 認証を有効にします。

コマンド デフォルト

デフォルトでは、クライアントのセキュア Web（https）認証は有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config network web-auth secureweb disable コマンドを使用してクライアントのセキュア Web（https）認証を設定する場合、Cisco WLC をリブートして変更を適用する必要があります。

次に、クライアントに対してセキュア Web（https）認証を有効にする例を示します。

```
(Cisco Controller) > config network web-auth secureweb enable
```

関連コマンド

show network summary

config network web-auth https-redirect

Web 認証クライアントの HTTPS リダイレクション サポートを設定するには、**config network web-auth https-redirect** コマンドを使用します。

config network web-auth https-redirect {**enable** | **disable**}

構文の説明

enable	Web 認証クライアントのセキュア リダイレクション（HTTPS）を有効にします。
disable	Web 認証クライアントのセキュア リダイレクション（HTTPS）を無効にします。

コマンド デフォルト

このコマンドは、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
8.0	このコマンドはリリース 8.0 で導入されました。

次に、Web 認証クライアントのプロキシのリダイレクションのサポートを有効にする例を示します。

```
(Cisco Controller) > config network web-auth https-redirect enable
```

関連コマンド

show network summary

config network webcolor

コントローラ GUI の Web カラー テーマを設定するには、**config network webcolor** コマンドを使用します。

config network webcolor {**default** | **red**}

構文の説明

default	コントローラ GUI のデフォルト Web カラー テーマを指定します。
red	コントローラ GUI の Web カラー テーマを赤に指定します。

コマンド デフォルト

default

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

コントローラ CLI から Web カラー テーマを変更した場合、変更を適用するにはコントローラ GUI をリロードする必要があります。

次に、コントローラ GUI の Web インターフェイスの色を赤に設定する例を示します。

```
(Cisco Controller) > config network webcolor red
```

config network webmode

Web モードを有効または無効にするには、**config network webmode** コマンドを使用します。

config network webmode {**enable** | **disable**}

構文の説明

enable	Webインターフェイスをイネーブルにします。
disable	Web インターフェイスをディセーブルにします。

コマンド デフォルト

Web モードのデフォルト値は **enable** です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web インターフェイス モードを無効にする例を示します。

```
(Cisco Controller) > config network webmode disable
```

関連コマンド

show network summary

config network web-auth

ネットワーク レベルの Web 認証オプションを設定するには、**config network web-auth** コマンドを使用します。

config network web-auth {**port** *port-number*} | {**proxy-redirect** {**enable** | **disable**}}

構文の説明

port	Web 認証リダイレクション用に追加ポートを設定します。
port-number	ポート番号（0 ～ 65535）。
proxy-redirect	Web 認証クライアントのプロキシ リダイレクション サポートを設定します。
enable	Web 認証クライアントのプロキシ リダイレクション サポートをイネーブルにします。 （注） Web 認証プロキシのリダイレクションは、ポート 80、8080、および 3128 に加え、ユーザ定義のポート 345 に対してイネーブルになります。
disable	Web 認証クライアントのプロキシ リダイレクション サポートをディセーブルにします。

コマンド デフォルト

ネットワーク レベルの Web 認証のデフォルト値は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

設定を有効にするには、システムをリセットする必要があります。

次に、Web 認証クライアントのプロキシのリダイレクションのサポートを有効にする例を示します。

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

関連コマンド

show network summary

show run-config

config qos protocol-type

config network zero-config

ブリッジのアクセス ポイントの ZeroConfig サポートを設定するには、**config network zero-config** コマンドを使用します。

config network zero-config {**enable** | **disable**}

構文の説明

enable	ブリッジのアクセス ポイントの ZeroConfig サポートをイネーブルにします。
disable	ブリッジのアクセス ポイントの ZeroConfig サポートをディセーブルにします。

コマンド デフォルト

ブリッジのアクセス ポイントの ZeroConfig サポートは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ブリッジのアクセス ポイントの ZeroConfig サポートを有効にする例を示します。

```
(Cisco Controller) >config network zero-config enable
```

config network allow-old-bridge-aps

スイッチとアソシエートする古いブリッジ アクセス ポイントの機能を設定するには、**config network allow-old-bridge-aps** コマンドを使用します。

config network allow-old-bridge-aps {**enable** | **disable**}

構文の説明

enable	スイッチ アソシエーションをイネーブルにします。
disable	スイッチ アソシエーションをディセーブルにします。

コマンド デフォルト

スイッチ アソシエーションは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、古いブリッジアクセス ポイントをスイッチに関連付けるように設定する例を示します。

```
(Cisco Controller) > config network allow-old-bridge-aps enable
```

config network ap-discovery

AP ディスカバリ応答で NAT IP を有効または無効にするには、**config network ap-discovery** コマンドを使用します。

config network ap-discovery nat-ip-only {**enable** | **disable**}

構文の説明

enable	NAT IP の使用をディスカバリ応答でのみイネーブルにします。
disable	ディスカバリ応答での NAT IP および非 NAT IP の両方の使用をイネーブルにします。

コマンド デフォルト

NAT IP の使用がディスカバリ応答でのみ有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config interface nat-address management コマンドが設定されている場合、このコマンドによって、CAPWAP ディスカバリ応答で送信されるアドレスが制御されます。

すべての AP がコントローラの NAT ゲートウェイの外側にある場合、**config network ap-discovery nat-ip-only enable** コマンドを入力して、管理 NAT アドレスのみを送信します。

コントローラが、NAT ゲートウェイの外部と内部の両方に AP を持つ場合、**config network ap-discovery nat-ip-only disable** コマンドを入力して、管理 NAT アドレスと管理内部アドレスの両方を送信します。AP が取り残されないように、**config ap link-latency disable all** コマンドを必ず入力してください。

次に、AP ディスカバリ応答で NAT IP を有効にする例を示します。

```
(Cisco Controller) > config network ap-discovery nat-ip-only enable
```

config network ap-fallback

Cisco Lightweight アクセス ポイントのフォールバックを設定するには、**config network ap-fallback** コマンドを使用します。

config network ap-fallback {**enable** | **disable**}

構文の説明

enable	Cisco Lightweight アクセス ポイントのフォール バックをイネーブルにします。
disable	Cisco Lightweight アクセス ポイントのフォール バックをディセーブルにします。

コマンド デフォルト

Cisco Lightweight アクセス ポイントのフォール バックは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco Lightweight アクセス ポイントのフォール バックを有効にする例を示します。

```
(Cisco Controller) > config network ap-fallback enable
```

config network ap-priority

Lightweight アクセス ポイントを優先するオプションを有効または無効にして、コントローラ障害後にコントローラが先着順ではなく優先順位によって再認証されるようにするには、**config network ap-priority** コマンドを使用します。

config network ap-priority {**enable** | **disable**}

構文の説明

enable	Lightweight アクセス ポイントの優先順位による再認証をイネーブルにします。
disable	Lightweight アクセス ポイントの優先順位による再認証をディセーブルにします。

コマンド デフォルト

Lightweight アクセス ポイントの優先順位による再認証は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Lightweight アクセス ポイントの優先順位による再認証を有効にする例を示します。

```
(Cisco Controller) > config network ap-priority enable
```

config network apple-talk

AppleTalk ブリッジを設定するには、**config network apple-talk** コマンドを使用します。

config network apple-talk {**enable** | **disable**}

構文の説明

enable	AppleTalk のブリッジをイネーブルにします。
disable	AppleTalk のブリッジをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、AppleTalk のブリッジを設定する例を示します。

```
(Cisco Controller) > config network apple-talk enable
```

config network bridging-shared-secret

ブリッジの共有キーを設定するには、**config network bridging-shared-secret** コマンドを使用します。

config network bridging-shared-secret *shared_secret*

構文の説明

shared_secret	ブリッジの共有キーの文字列。文字列には 10 バイトまで使用できます。

コマンド デフォルト

ブリッジの共有キーは、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドにより、スイッチに接続するメッシュ アクセス ポイントのバックホール ユーザ データを暗号化する共有キーが作成されます。

このコマンドを機能させるには、zero touch configuration をイネーブルにしておく必要があります。

次に、ブリッジの共有キーの文字列「shhh1」を設定する例を示します。

```
(Cisco Controller) > config network bridging-shared-secret shhh1
```

関連コマンド

show network summary

config network master-base

Cisco ワイヤレス LAN コントローラをアクセス ポイントのデフォルト マスターとして有効または無効にするには、**config network master-base** コマンドを使用します。

config network master-base {**enable** | **disable**}

構文の説明

enable	Cisco Lightweight アクセス ポイントのデフォルト マスターとして機能している Cisco ワイヤレス LAN コントローラをイネーブルにします。
disable	Cisco Lightweight アクセス ポイントのデフォルト マスターとして機能している Cisco ワイヤレス LAN コントローラをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

この設定はネットワークのインストール時にのみ使用され、初期ネットワーク設定後は無効にする必要があります。通常、マスター Cisco ワイヤレス LAN コントローラは展開済みネットワークでは使用されないため、マスター Cisco ワイヤレス LAN コントローラの設定は 6.0.199.0 以降のリリースから保存できます。

次に、デフォルト マスターとして Cisco ワイヤレス LAN コントローラを有効にする例を示します。

```
(Cisco Controller) > config network master-base enable
```

config network oeap-600 dual-rlan-ports

Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、ポート 4 に加えて、リモート LAN ポートとしても機能するように設定するには、**config network oeap-600 dual-rlan-ports** コマンドを使用します。

config network oeap-600 dual-rlan-ports {**enable** | **disable**}

構文の説明

enable	Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、ポート 4 に加えて、リモートLANポートとしても機能できるようにします。
disable	Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネットポート3をリセットして、ローカルLANポートとして機能するようにします。

コマンド デフォルト

Cisco 600 シリーズ OEAP のイーサネット ポート 3 がリセットされます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、リモートの LAN ポートとして機能できるようにする例を示します。

```
(Cisco Controller) > config network oeap-600 dual-rlan-ports enable
```

config network oeap-600 local-network

Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスを設定するには、**config network oeap-600 local-network** コマンドを使用します。

config network oeap-600 local-network {**enable** | **disable**}

構文の説明

enable	Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスをイネーブルにします。
disable	Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスをディセーブルにします。

コマンド デフォルト

Cisco 600 シリーズ OEAP のローカル ネットワークへのアクセスは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスを有効にする例を示します。

```
(Cisco Controller) > config network oeap-600 local-network enable
```

config network otap-mode

Cisco Lightweight アクセス ポイントの無線プロビジョニング（OTAP）を有効または無効にするには、**config network otap-mode** コマンドを使用します。

config network otap-mode {**enable** | **disable**}

構文の説明

enable	OTAP プロビジョニングをイネーブルにします。
disable	OTAP プロビジョニングをディセーブルにします。

コマンド デフォルト

OTAP プロビジョニングは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、OTAP プロビジョニングを無効にする例を示します。

```
(Cisco Controller) >config network otap-mode disable
```

config network zero-config

ブリッジのアクセス ポイントの ZeroConfig サポートを設定するには、**config network zero-config** コマンドを使用します。

config network zero-config {**enable** | **disable**}

構文の説明

enable	ブリッジのアクセス ポイントの ZeroConfig サポートをイネーブルにします。
disable	ブリッジのアクセス ポイントの ZeroConfig サポートをディセーブルにします。

コマンド デフォルト

ブリッジのアクセス ポイントの ZeroConfig サポートは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ブリッジのアクセス ポイントの ZeroConfig サポートを有効にする例を示します。

```
(Cisco Controller) >config network zero-config enable
```

config nmsp notify-interval measurement

コントローラの Network Mobility Services Protocol (NMSP) 通知間隔値をネットワーク内の遅延に対応するように変更するには、**config nmsp notify-interval measurement** コマンドを使用します。

config nmsp notify-interval measurement {**client** | **rfid** | **rogue**} *interval*

構文の説明

client	クライアントの間隔を変更します。
rfid	アクティブな無線周波数ID（RFID）タグの間隔を変更します。
rogue	不正なアクセス ポイントおよび不正なクライアントの間隔を変更します。
interval	時間間隔。範囲は 1 ～ 30 秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

コントローラとロケーション アプライアンスとの通信には、TCP ポート 16113 が使用されます。コントローラとロケーションアプライアンスの間にファイアウォールがある場合は、NMSP が機能するにはこのポートが開いている（ブロックされていない）ことが必要です。

次に、アクティブな RFID タグの NMSP 通知間隔を 25 秒に変更する例を示します。

```
(Cisco Controller) > config nmsp notify-interval measurement rfid 25
```

関連コマンド

clear locp statistics

clear nmsp statistics

show nmsp notify-interval summary

show nmsp statistics

show nmsp status

config paging

ページのスクロールを有効または無効にするには、**config paging** コマンドを使用します。

config paging {**enable** | **disable**}

構文の説明

enable	ページのスクロールをイネーブルにします。
disable	ページのスクロールをディセーブルにします。

コマンド デフォルト

デフォルトでは、ページのスクロールは有効になっています。

使用上のガイドライン

ページのスクロールを無効にした状態で膨大な数の出力行を生成するコマンドを実行すると、SSH/Telnet 接続またはコンソールでのユーザ セッションが終了する可能性があります。

次に、ページのスクロールを有効にする例を示します。

```
(Cisco Controller) > config paging enable
```

関連コマンド

show run-config

config passwd-cleartext

プレーン テキストでのパスワードの一時的な表示を有効または無効にするには、**config passwd-cleartext** コマンドを使用します。

config passwd-cleartext {**enable** | **disable**}

構文の説明

enable	プレーン テキストでのパスワードの表示をイネーブルにします。
disable	プレーンテキストでのパスワードの表示をディセーブルにします。

コマンド デフォルト

デフォルトでは、プレーン テキストでのパスワードの一時的な表示は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

show run-config コマンドを使用する際にユーザが割り当てたパスワードをクリア テキストで表示する場合には、このコマンドを無効にする必要があります。

このコマンドを実行するには、admin パスワードを入力する必要があります。このコマンドは、この特定のセッションだけで有効です。リブート後には保存されません。

次に、プレーン テキストでパスワードの表示を有効にする例を示します。

```
(Cisco Controller) > config passwd-cleartext enable
The way you see your passwds will be changed
You are being warned.
Enter admin password:
```

関連コマンド

show run-config

config policy

Cisco ワイヤレス LAN コントローラ（WLC）でネイティブ プロファイリング ポリシーを設定するには、**config policy** コマンドを使用します。

config policy*policy_name* {**action** {**acl** {**enable** | **disable**} *acl_name* | {**average-data-rate** | **average-realtime-rate** | **burst-data-rate** | **burst-realtime-rate** | **qos** | **session-timeout** | **sleeping-client-timeout** | **avc-profile-name** {**enable** *avc_profile_name* | **disable**} | **vlan**} {**enable** | **disable**}} | **active** {**add hours** *start _time end _time* **days** *day* | **delete days** *day*} | **create** | **delete** | **match** {**device-type** {**add** | **delete**} *device-type* | **eap-type** {**add** | **delete**} {**eap-fast** | **eap-tls** | **leap** | **peap**} | **role** {*role_name* | **none**}}

構文の説明

policy_name	プロファイリング ポリシーの名前。
action	ポリシーのアクションを設定します。
acl	ポリシーの ACL を設定します。
enable	ポリシーのアクションを有効にします。
disable	ポリシーのアクションを無効にします。
acl_name	ACL の名前です。
average-data-rate	QoS 平均データ レートを設定します。
average-realtime-rate	QoS 平均リアルタイム レートを設定します。
burst-data-rate	QoS バースト データ レートを設定します。
burst-realtime-rate	QoSバーストリアルタイム レートを設定します。
qos	ポリシーの QoS アクションを設定します。
session-timeout	ポリシーのセッション タイムアウト アクションを設定します。
sleeping-client-timeout	ポリシーのスリープ クライアント タイムアウトを設定します。
avc-profile-name	ポリシーで AVC プロファイルを設定します。
vlan	ポリシーの VLAN アクションを設定します。
active	ポリシーのアクティブな時間および日を設定します。
add	アクティブな時間と日を追加します。
hours	ポリシーのアクティブな時間を設定します。

Start Time	ポリシーの開始時間。
End Time	ポリシーの終了時間。
days	ポリシーが機能する必要がある日を設定します。
day	曜日（**mon**、**tue**、**wed**、**thu**、**fri**、**sat**、**sun**など）。ポリシーが毎日または平日に機能するように daily または weekdays を指定することもできます。
delete	アクティブな時間と日を削除します。
create	ポリシーを作成します。
match	ポリシーの一致基準を設定します。
device-type	一致するデバイス タイプを設定します。
device-type	ポリシーを適用する必要があるデバイスタイプ。1 つのポリシーに最大 16 のデバイス タイプを設定できます。
eap-type	拡張可能認証プロトコル（EAP）タイプを一致基準として設定します。
eap-fast	EAP タイプを EAP セキュア トンネル経由フレキシブル認証（FAST）として設定します。
eap-tls	EAP タイプを EAP トランスポート層セキュリティ（TLS）として設定します。
leap	EAP タイプを Lightweight EAP（LEAP）として設定します。
peap	EAP タイプを Protected EAP（PEAP）として設定します。
role	ユーザのユーザ タイプまたはユーザ グループを設定します。
role_name	ユーザのユーザタイプまたはユーザグループ（学生、従業員など）。 ポリシーごとに 1 つのロールのみを設定できます。
none	ユーザのユーザ タイプまたはユーザ グループを設定しません。

コマンド デフォルト

Cisco WLC にはネイティブのプロファイリング ポリシーはありません。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

設定できるポリシーの最大数は 64 です。

次に、ポリシーのロールを設定する例を示します。

```
(Cisco Controller) > config policy student_policy role student
```

config port adminmode

特定のコントローラ ポートまたはすべてのポートの管理モードを有効または無効にするには、**config port adminmode** コマンドを使用します。

config port adminmode {**all** | *port*} {**enable** | **disable**}

構文の説明

all	すべてのポートを設定します。
port	ポート番号。
enable	指定したポートをイネーブルにします。
disable	指定したポートをディセーブルにします。

コマンド デフォルト

イネーブル

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、ポート 8 を無効にする例を示します。

```
(Cisco Controller) > config port adminmode 8 disable
```

次に、すべてのポートを有効にする例を示します。

```
(Cisco Controller) > config port adminmode all enable
```

config port autoneg

10/100BASE-Tイーサネット ポートで物理ポート自動ネゴシエーションを設定するには、**config port autoneg** コマンドを使用します。

config port autoneg {**all** | *port*} {**enable** | **disable**}

構文の説明

all	すべてのポートを設定します。
port	ポート番号。
enable	指定したポートをイネーブルにします。
disable	指定したポートをディセーブルにします。

コマンド デフォルト

デフォルトでは、すべてのポートの自動ネゴシエーションが有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config port physicalmode コマンドを使用して物理モードの手動設定を行う前に、ポート自動ネゴシエーションを無効にする必要があります。**config port autoneg** コマンドは、**config port physicalmode** コマンドを使用して行った設定を上書きします。

次に、前面パネルのすべてのイーサネット ポートで物理ポートの自動ネゴシエーションをオンにする例を示します。

```
(Cisco Controller) > config port autoneg all enable
```

次に、前面パネルのイーサネット ポート 19 で物理ポートの自動ネゴシエーションを無効にする例を示します。

```
(Cisco Controller) > config port autoneg 19 disable
```

config port linktrap

特定のコントローラ ポートまたはすべてのポートのリンク アップ/ダウン トラップを有効または無効にするには、**config port linktrap** コマンドを使用します。

config port linktrap {**all** | *port*} {**enable** | **disable**}

構文の説明

all	すべてのポートを設定します。
port	ポート番号。
enable	指定したポートをイネーブルにします。
disable	指定したポートをディセーブルにします。

コマンド デフォルト

特定のコントローラ ポートまたはすべてのポートのダウンリンク トラップのデフォルト値は有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、ポート 8 のトラップを無効にする例を示します。

```
(Cisco Controller) > config port linktrap 8 disable
```

次に、すべてのポートのトラップを有効にする例を示します。

```
(Cisco Controller) > config port linktrap all enable
```

config port multicast appliance

特定のコントローラ ポートまたはすべてのポートのマルチキャスト アプライアンス サービスを有効または無効にするには、**config port multicast appliance** コマンドを使用します。

config port multicast appliance {**all** | *port*} {**enable** | **disable**}

構文の説明

all	すべてのポートを設定します。
port	ポート番号。
enable	指定したポートをイネーブルにします。
disable	指定したポートをディセーブルにします。

コマンド デフォルト

特定のコントローラ ポートまたはすべてのポートのデフォルトのマルチキャスト アプライアンス サービスは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのポートでマルチキャスト アプライアンス サービスを有効にする例を示します。

```
(Cisco Controller) > config port multicast appliance all enable
```

次に、ポート 8 でマルチキャスト アプライアンス サービスを無効にする例を示します。

```
(Cisco Controller) > config port multicast appliance 8 disable
```

config prompt

CLI システム プロンプトを変更するには、**config prompt** コマンドを使用します。

config prompt *prompt*

構文の説明

prompt	二重引用符で囲まれた新しい CLI システム プロンプト。プロンプトには最大 31 文字の英数字を使用できます。また、大文字と小文字は区別されます。

コマンド デフォルト

システム プロンプトは起動ウィザードを使用して設定します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

システム プロンプトはユーザ定義変数であるため、このドキュメントの他の項では割愛します。

次に、Cisco 4400 への CLI システム プロンプトを変更する例を示します。

```
(Cisco Controller) > config prompt "Cisco 4400"
```

config qos average-data-rate

ユーザごとまたはサービス セット ID（SSID）ごとに TCP トラフィックの平均データ レートを Kbps 単位で定義するには、**config qos average-data-rate** コマンドを使用します。

config qos average-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

構文の説明

bronze	キューの平均データ レートを bronze に指定します。
silver	キューの平均データ レートを silver に指定します。
gold	キューの平均データ レートを gold に指定します。
platinum	キューの平均データ レートを platinum に指定します。
per-ssid	無線ごとの SSID のレート制限を設定します。すべてのクライアントの混合トラフィックはこの制限を超えないようになります。
per-client	SSID に関連付けられた各クライアントのレート制限を設定します。
downstream	ダウンストリーム トラフィックのレート制限を設定します。
upstream	アップストリーム トラフィックのレート制限を設定します。
rate	ユーザ 1 人あたりの TCP トラフィックの平均データ レート。値は、0 ～ 51,2000 Kbps です。値に 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、SSID ごとにキューの平均データ レート 0 Kbps を gold に設定する例を示します。

```
(Cisco Controller) > config qos average-data-rate gold per ssid downstream 0
```

関連コマンド

config qos burst-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config wlan override-rate-limit

config qos average-realtime-rate

ユーザごとまたはサービス セット ID（SSID）ごとに UDP トラフィックの平均リアルタイム データ レートを Kbps 単位で定義するには、**config qos average-realtime-rate** コマンドを使用します。

config qos average-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

構文の説明

bronze	キューの平均リアルタイム データ レートを bronze に指定します。
silver	キューの平均リアルタイム データ レートを silver に指定します。
gold	キューの平均リアルタイム データ レートを gold に指定します。
platinum	キューの平均リアルタイム データ レートを platinum に指定します。
per-ssid	無線ごとの SSID のレート制限を設定します。すべてのクライアントの混合トラフィックはこの制限を超えないようになります。
per-client	SSID に関連付けられた各クライアントのレート制限を設定します。
downstream	ダウンストリーム トラフィックのレート制限を設定します。
upstream	アップストリーム トラフィックのレート制限を設定します。
rate	ユーザ 1 人あたりの UDP トラフィックの平均リアルタイム データ レート。値は、0 ～ 51,2000 Kbps です。値に 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、キューの平均リアルタイムの実際のレートを gold に設定する例を示します。

```
(Cisco Controller) > config qos average-realtime-rate gold per ssid downstream 10
```

関連コマンド

config qos average-data-rate

config qos burst-data-rate

config qos burst-realtime-rate

config wlan override-rate-limit

config qos burst-data-rate

ユーザごとまたはサービス セット ID（SSID）ごとに TCP トラフィックのピーク データ レートを Kbps 単位で定義するには、**config qos burst-data-rate** コマンドを使用します。

config qos burst-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

構文の説明

bronze	キューのピーク データ レートを bronze に指定します。
silver	キューのピーク データ レートを silver に指定します。
gold	キューのピーク データ レートを gold に指定します。
platinum	キューのピーク データ レートを platinum に指定します。
per-ssid	無線ごとの SSID のレート制限を設定します。すべてのクライアントの混合トラフィックはこの制限を超えないようになります。
per-client	SSID に関連付けられた各クライアントのレート制限を設定します。
downstream	ダウンストリーム トラフィックのレート制限を設定します。
upstream	アップストリーム トラフィックのレート制限を設定します。
rate	ユーザ 1 人あたりの TCP トラフィックのピーク データ レート。値は、0 ～ 51,2000 Kbps です。値に 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、キューのピーク レート 30000 kbps を gold に設定する例を示します。

```
(Cisco Controller) > config qos burst-data-rate gold per ssid downstream 30000
```

関連コマンド

config qos average-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config wlan override-rate-limit

config qos burst-realtime-rate

ユーザごとまたはサービス セット ID（SSID）ごとに UDP トラフィックのバースト リアルタイム データ レートを Kbps 単位で定義するには、**config qos burst-realtime-rate** コマンドを使用します。

config qos burst-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} { **per-ssid** | **per-client** } { **downstream** | **upstream** } *rate*

構文の説明

bronze	キューのバーストリアルタイムデータ レートを bronze に指定します。
silver	キューのバーストリアルタイムデータ レートを silver に指定します。
gold	キューのバーストリアルタイムデータ レートを gold に指定します。
platinum	キューのバーストリアルタイムデータ レートを platinum に指定します。
per-ssid	無線ごとの SSID のレート制限を設定します。すべてのクライアントの混合トラフィックはこの制限を超えないようになります。
per-client	SSID に関連付けられた各クライアントのレート制限を設定します。
downstream	ダウンストリーム トラフィックのレート制限を設定します。
upstream	アップストリーム トラフィックのレート制限を設定します。
rate	ユーザ 1 人あたりの UDP トラフィックのバースト リアルタイム データ レート。値は、0 ～ 51,2000 Kbps です。値に 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、キューのバースト リアルタイムの実際のレート 2000 kbps を gold に設定する例を示します。

```
(Cisco Controller) > config qos burst-realtime-rate gold per ssid downstream  2000
```

関連コマンド

config qos average-data-rate

config qos burst-data-rate

config qos average-realtime-rate

config wlan override-rate-limit

config qos description

プロファイルの説明を変更するには、**config qos description** コマンドを使用します。

config qos description {**bronze** | **silver** | **gold** | **platinum**} *description*

構文の説明

bronze	キューの QoS プロファイルの説明を bronze に指定します。
silver	キューの QoS プロファイルの説明を silver に指定します。
gold	キューの QoS プロファイルの説明を gold に指定します。
platinum	キューの QoS プロファイルの説明を platinum に指定します。
description	QoS プロファイルの説明。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、キューの QoS プロファイルの説明「description」を gold に設定する例を示します。

```
(Cisco Controller) > config qos description gold abc
```

関連コマンド

show qos average-data-rate

config qos burst-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config qos max-rf-usage

config qos fastlane

WLAN ごとに Fastlane QoS 機能を有効にするには、**config qos fastlane** コマンドを使用します。

config qos fastlane {**enable** | **disable**} *wlan-id*

構文の説明

enable	WLAN ごとに Fastlane QoS を有効にします。
disable	WLAN ごとに Fastlane QoS を無効にします。
wlan-id	WLAN 識別子。

コマンド デフォルト

Fastlane は設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
8.3	このコマンドが導入されました。

例

次に、WLAN ごとに Fastlane QoS を設定する例を示します。

```
Controller(config)# config qos fastlane enable 1
```

config qos fastlane disable global

Fastlane QoS 機能をグローバルに無効にするには、**config qos fastlane disable global** コマンドを使用します。

config qos fastlane disable global

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
8.3	このコマンドが導入されました。

使用上のガイドライン

このコマンドを実行する前にすべての WLAN で Fastlane QoS が無効になっている必要があります。

例

次に、Apple ワイヤレス クライアントの Fastlane QoS をグローバルに無効にする例を示します。

```
Controller(config)# config qos fastlane disable global
```

config qos max-rf-usage

アクセス ポイント 1 つあたりの RF 利用率の最大パーセンテージを設定するには、**config qos max-rf-usage** コマンドを使用します。

config qos max-rf-usage {**bronze** | **silver** | **gold** | **platinum**} *usage_percentage*

構文の説明

bronze	キューの RF 使用率の最大パーセントを bronze に指定します。
silver	キューの RF 使用率の最大パーセントを silver に指定します。
gold	キューの RF 使用率の最大パーセントを gold に指定します。
platinum	キューの RF 使用率の最大パーセントを platinum に指定します。
usage-percentage	RF 利用率の最大パーセンテージ。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、キューの RF 使用率の最大パーセントを gold に指定する例を示します。

```
(Cisco Controller) > config qos max-rf-usage gold 20
```

関連コマンド

show qos description

config qos average-data-rate

config qos burst-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config qos dot1p-tag

プロファイル内に分類されるパケットに関連付けられた優先タグの最大値（0 ～ 7）を定義するには、**config qos dot1p-tag** コマンドを使用します。

config qos dot1p-tag {**bronze** | **silver** | **gold** | **platinum**} *dot1p_tag*

構文の説明

bronze	キューの QoS 802.1p タグを bronze に設定します。
silver	キューの QoS 802.1p タグを silver に設定します。
gold	キューの QoS 802.1p タグを gold に設定します。
platinum	キューの QoS 802.1p タグを platinum に設定します。
dot1p_tag	1 ～ 7 の間の Dot1p タグの値。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、dot1p タグの値を 5 に設定して、キューの QoS 802.1p タグを gold に設定する例を示します。

```
(Cisco Controller) > config qos dot1p-tag gold 5
```

関連コマンド

show qos queue_length all

config qos protocol-type

config qos priority

QoSプロファイルをWLANに割り当てるときに、ユニキャストとマルチキャストのトラフィックに最大およびデフォルトの QoS レベルを定義するには、**config qos priority** コマンドを使用します。

config qos priority {**bronze** | **silver** | **gold** | **platinum**} {*maximum-priority* | *default-unicast-priority* | *default-multicast-priority*}

構文の説明

bronze	WLANのBronzeプロファイルを指定します。
silver	WLAN の Silver プロファイルを指定します。
gold	WLAN の Gold プロファイルを指定します。
platinum	WLAN の Platinum プロファイルを指定します。
maximum-priority	最大QoS優先度。次のいずれかを指定します。 • besteffort • background • video • voice
default-unicast-priority	デフォルト ユニキャストの優先度。次のいずれかを指定します。 • besteffort • background • video • voice
default-multicast-priority	デフォルト マルチキャストの優先度。次のいずれかを指定します。 • besteffort • background • video • voice

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

最大優先度レベルは、デフォルトのユニキャストとマルチキャストの優先度レベル以上にする必要があります。

次に、最大優先度として voice、デフォルト ユニキャスト優先度として video、およびデフォルト マルチキャスト優先度として besteffort を設定した WLAN の gold プロファイルに QoS 優先度を設定する例を示します。

```
(Cisco Controller) > config qos priority gold voice video besteffort
```

関連コマンド

config qos protocol-type

config qos protocol-type

プロファイル内に分類されるパケットに関連付けられた優先タグの最大値（0 ～ 7）を定義するには、**config qos protocol-type** コマンドを使用します。

config qos protocol-type {**bronze** | **silver** | **gold** | **platinum**} {**none** | *dot1p*}

構文の説明

bronze	キューの QoS 802.1p タグを bronze に設定します。
silver	キューの QoS 802.1p タグを silver に設定します。
gold	キューの QoS 802.1p タグを gold に設定します。
platinum	キューの QoS 802.1p タグを platinum に設定します。
none	特定のプロトコルが割り当てられていないときに指定します。
dot1p	dot1p タイプのプロトコルが割り当てられているときに指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、QoS プロトコル タイプを silver に設定する例を示します。

```
(Cisco Controller) > config qos protocol-type silver dot1p
```

関連コマンド

show qos queue_length all

config qos dot1p-tag

config qos queue_length

アクセス ポイントがキュー内に保持するパケットの最大数を指定するには、**config qos queue_length** コマンドを使用します。

config qos queue_length {**bronze** | **silver** | **gold** | **platinum**} *queue_length*

構文の説明

bronze	キューの QoS 長を bronze に指定します。
silver	キューの QoS 長を silver に指定します。
gold	キューの QoS 長を gold に指定します。
platinum	キューの QoS 長を platinum に指定します。
queue_length	キューの長さの最大値（10 ～ 255）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、最大キュー長の値を 12 に設定して、キューの QoS 長を「gold」に設定する例を示します。

```
(Cisco Controller) > config qos queue_length gold 12
```

関連コマンド

show qos

config qos qosmap

QoS マップを設定するには、**config qos qosmap** コマンドを使用します。

config qos qosmap {**enable** | **disable** | **default** }

構文の説明

enable	QoS マップ機能を有効にします。
disable	QoS マップ機能を無効にします。
default	デフォルトの QoS マップをリセットします。 QoSマップの値が255（デフォルト）にリセットされます。また、DSCP UP 例外が存在しなければ追加します。DSCP UP 値をクリアするには、 **config qos qosmap clear-all** コマンドを入力します。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、QoS マップを有効にする例を示します。

```
(Cisco Controller) > config qos qosmap enable
```

config qos qosmap up-to-dscp-map

UP の DSCP 範囲を設定するには、**config qos qosmap** コマンドを使用します。

config qos qosmap up-to-dscp-map {*up dscp-default dscp-start dscp-end*}

構文の説明

up-to-dscp-map	UP の DSCP 範囲を設定します。
up	ワイヤレス UP 値。
dscp-default	この UP のデフォルト DSCP 値。
dscp-start	DSCP の開始範囲。範囲は 0 ~ 63 です。
dscp-end	DSCP の終了範囲。範囲は 0 ~ 63 です。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、UP の DSCP 範囲を設定する例を示します。

```
(Cisco Controller) > config qos qosmap up-to-dscp-map 2 3 5 20
```

config qos qosmap dscp-to-up-exception

DSCP 例外を設定するには、**config qos qosmap** コマンドを使用します。

config qos qosmap dscp-to-up-exception {*dscp up* }

構文の説明

dscp-to-up-exception	DSCP 例外の設定を許可します。
dscp	UP 値の例外 DSCP 値。
up	ワイヤレス ユーザ優先度（UP）値へのリンク。

次に、DSCP 例外を設定する例を示します。

```
(Cisco Controller) > config qos qosmap dscp-to-up-exception 3 1
```

config qos qosmap delete-dscp-exception

DSCP 例外を削除するには、**config qos qosmap** コマンドを使用します。

config qos qosmap delete-dscp-exception *dscp*

構文の説明

delete-dscp-exception	DSCP の例外を削除します。
dscp	UP の DSCP の例外

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、DSCP の例外を削除する例を示します。

```
(Cisco Controller) > config qos qosmap delete-dscp-exception 23
```

config qos qosmap clear-all

QoS マップからすべての例外を削除するには、**config qos qosmap** コマンドを使用します。

config qos qosmap clear-all

構文の説明		
	clear-all	すべての例外を削除します。

コマンド履歴		
	リリース	変更内容
	8.1	このコマンドが導入されました。

次に、QoS マップからすべての例外をクリアする例を示します。

```
(Cisco Controller) > config qos qosmap clear-all
```

config qos qosmap trust dscp upstream

クライアントの DSCP を使用してアップ ストリーム パケットをマーキングするには、**config qos qosmap** コマンドを使用します。

config qos qosmap trust-dscp-upstream {**enable** | **disable**}

構文の説明

trust-dscp-upstream	クライアントの DSCP に基づいてアップストリーム パケットがマーキングされます。
enable	クライアントの DSCP を使用したアップストリームパケットのマーキングを有効にします。
disable	クライアントの DSCP を使用したアップストリームパケットのマーキングを無効にします。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、クライアントの DSCP に基づいたパケット マーキングを有効にする例を示します。

```
(Cisco Controller) > config qos qosmap trust-dscp-upstream enable
```