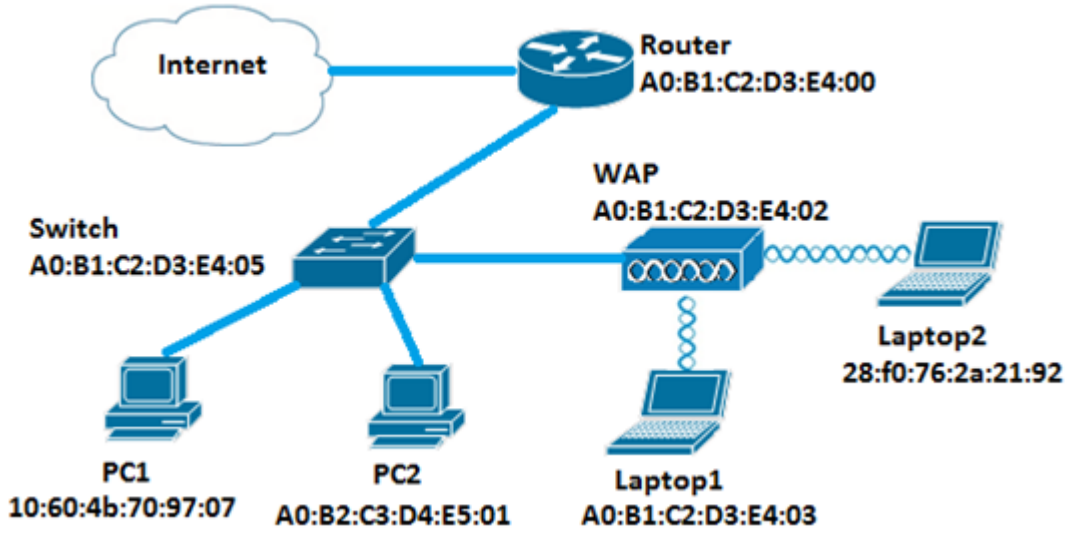
WAP125 および WAP581 の MAC ACL を設定して下さい

概要

Media Access Control（MAC）アクセス コントロール リスト（ACL）はレイヤ2 ACL です。 各 ACL はワイヤレスアクセスポイント（WAP）受信されるトラフィックに適用される一組の規則です。 ルールはある特定のフィールド ã® ã³ã³ãã³ã がネットワークにアクセスを許可するか、または拒否するのに使用する必要があるかどうか規定 します。 ACL は送信元または 宛先MACアドレス、Virtual Local Area Network （VLAN; バーチャル LAN） 識別子（ID）、または Class of Service（CoS）のようなフレームのフィールドを点検するために設定することができます。 フレームが WAP デバイス ポートを入力するとき、フレームを点検し、フレームのコンテンツに対して ACL ルールをチェックします。 ルールのうちのどれかがコンテンツを一致する場合、割り当てか拒否処置はフレームでとられます。 MAC ACL をネットワークで『Devices』 を選択 するために設定することが一般的に ネットワークリソースにアクセスを許可するのに使用されています。

注: 作成される各ルールの終わりに暗黙の deny があります。



このシナリオでは PC1 を除いて WAP の後ろの Laptop2 にアクセスできることが、ネットワークのすべてのデバイスはできます。

目標

この技術情報は PC1 が WAP の後ろで Laptop2 にアクセスすることを防ぐために WAP125 か WAP581 アクセス ポイントの MAC ベースの ACL を設定する方法を示すことを向けます。

適当なデバイス

- WAP125
- WAP581

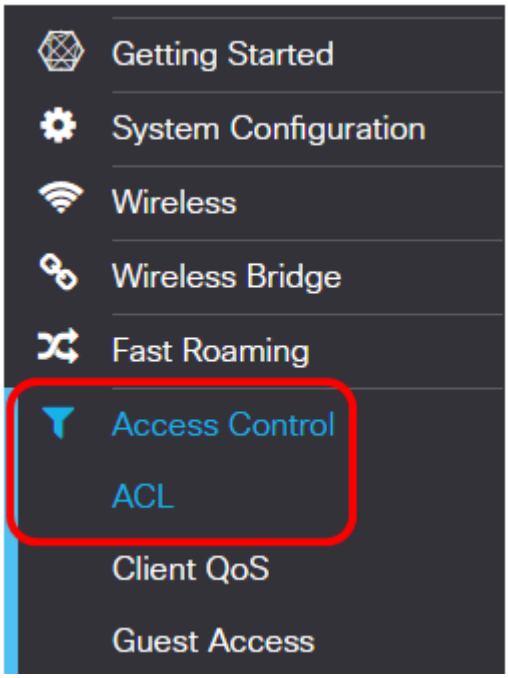
[Software Version]

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

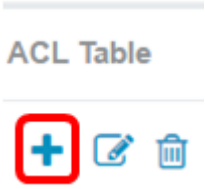
クライアント フィルタリストを設定して下さい

注: メニューオプションは WAP の正確なモデルによって使用していること変わるかもしれません。 イメージは下記の WAP125 から撮られます。

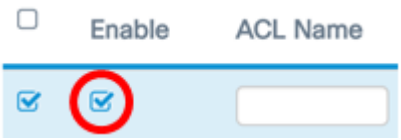
ステップ 1. WAP の Webベース ユーティリティへのログインは**アクセスコントロール > ACL を**選択し。



ステップ 2.ボタンを➕ クリックして下さい。



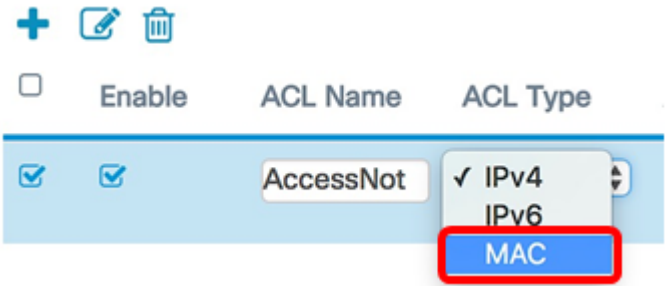
ステップ 3. ACL がアクティブであることを確認するために **Enable チェックボックスが**チェックされることを確認して下さい。 このオプションはデフォルトでチェックされます。



ステップ 4. ACL を識別するために *ACL Name フィールド*で ACL の名前を入力して下さい。

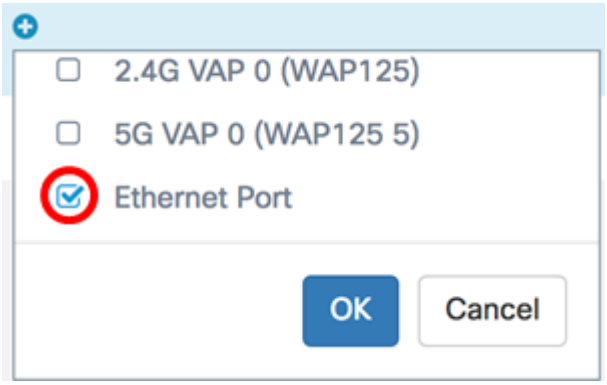
注: この例では、AccessNot は入ります。

ステップ 5. ACL 型ドロップダウン リストから **MAC** を選択して下さい。



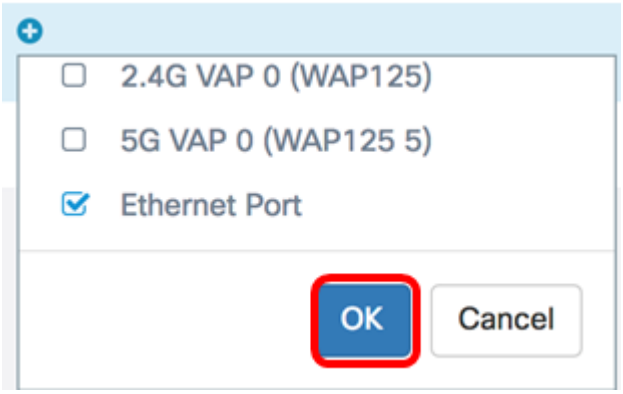
ステップ 6.ボタンを クリックし、関連するインターフェイス ドロップダウン リストからインターフェイスを選択して下さい。 オプションは次のとおりです:

- 2.4G VAP 0 （ SSID 名前 ）は 2.4 GHz バーチャルアクセス アクセス· ポイント （ VAP ）に—このオプション MAC ACL を適用します。 SSID 名前セクションは WAP で設定される SSID 名前によって変更するかもしれません。
- 5G VAP0 （ SSID 名前 ） —このオプションは 5 GHz VAP に MAC ACL を適用します。
- イーサネットポート—このオプションは WAP のイーサネットインターフェイスに MAC ACL を適用します。

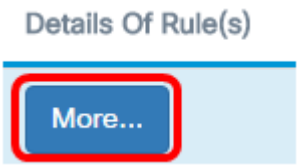


注: マルチプルインターフェイスは ACL に関連付けることができます。 ACL にインターフェイスを関連付けるために対応するインターフェイスのチェックボックスをチェックして下さい。 ACL からのインターフェイスを引き離すためにボックスのチェックを外して下さい。 この例では、イーサネットポートは ACL に対応づけられています。

ステップ 7. 『OK』 をクリック して下さい。



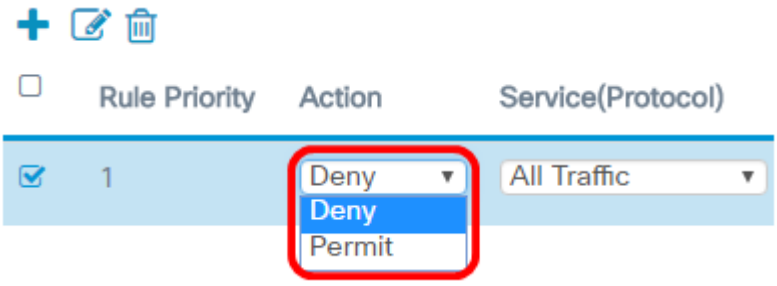
ステップ 8. ACL のパラメータを設定するために **More ボタンを**クリックして下さい。



ステップ 9.新しい＋ ルールを追加するためにボタンをクリックして下さい。

ステップ 10.処理 ドロップダウン リストから操作を選択して下さい。 オプションは次のとおりです:

- permit —このオプションはネットワークに接続するために ACL 条件を満たしたパケットを可能にします。
- 拒否—このオプションはからのネットワークに ACL 条件を接続満たしたパケットを防ぎます。



注: この例では、拒否は選択されます。

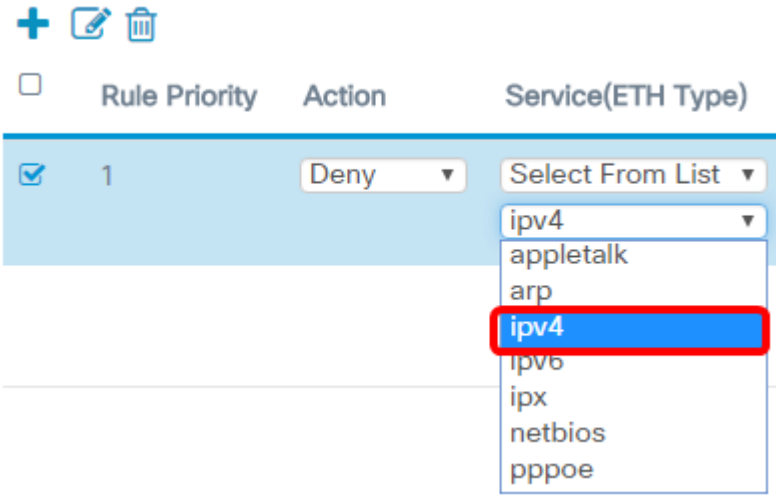
ステップ 11.サービス (プロトコル) ドロップダウン リストからフィルタリングされるべきサービスかプロトコルを選択して下さい。 オプションは次のとおりです:

- すべては ACL フィルタにマッチとして traffic —このオプションすべてのパケットを処理します。
- list —このオプションから ACL のためのフィルタとして AppleTalk、arp、ipv4、IPv6、IPX、NetBIOS および pppoe を選択することを許可します選択して下さい。 このオプションを選択する場合、ステップ 12 にスキップして下さい。
- カスタム—このオプションはパケットのためのフィルタとしてカスタム プロトコル 識別子を入力することを可能にします。 値は四桁 16進数です。 範囲は FFFF へ 0600 です。

注: この例では、**すべてのトラフィックは**選択されます。

ステップ 12： 『Select from List』 を選択 した場合（オプションの）、の次のオプション選択して下さい:

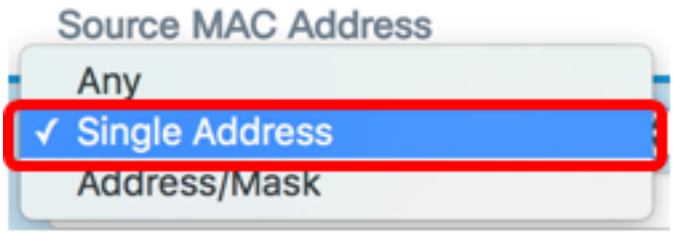
- AppleTalk —このオプションは ACL の文に基づいて AppleTalkパケットをフィルタリングします。 AppleTalk は Mac コンピュータのための Apple によって開発される一組のネットワーキングプロトコルです。 機能の 1 つはローカル エリア ネットワーク（LAN）がセントラルルータまたはサーバの必要なしで接続されるようにします。
- arp —このオプションは ACL の文に基づいてアドレス解決プロトコル（ARP）パケットをフィルタリングします。 ARP は IP アドレスへの MAC アドレスがマッピング される 表を維持します。
- ipv4 —このオプションは ACL の文に基づいて ipv4 パケットをフィルタリングします。
- IPv6 —このオプションは ACL の文に基づいて IPv6 パケットをフィルタリングします。 IPv6 はネットワークアドレッシングの IPv6 のサクセサです。
- IPX —このオプションは ACL の文に基づいて Internetwork Packet Exchange （IPX）パケットをフィルタリングします。 AppleTalk のように、IPX はまた独自のネットワーキングプロトコルです。 それは Novellクライアントおよびサーバを利用するネットワークを接続します。
- NetBIOS —このオプションはネットワーク ACL の文に基づいて基本的な入出力 システム（NetBIOS（NetBIOS over IP））パケットをフィルタリングします。 NetBIOS（NetBIOS over IP）別々のコンピューターのアプリケーションが通信ことそれらにサービスをできるために提供することによって通信するようにします。
- pppoe —このオプションは ACL の文に基づいて Point-to-Point Protocol over Ethernet（PPPoE）パケットをフィルタリングします。 それは Digital Subscriber Line（dsl） サービスで主に使用されます。



注: この例では、ipv4 は選択されます。

ステップ 13： 送信元MACアドレス ドロップダウン リストからの送信元MACアドレスを定義して下さい。 オプションは次のとおりです:

- —このオプションは WAP があらゆる MAC アドレスからパケットにフィルタを適用するようにします。
- 単一のアドレス—このオプションは WAP が特定のMACアドレスからパケットにフィルタを適用するようにします。
- アドレス/マスク—このオプションは WAP が MAC アドレスにパケットにフィルタおよび WAP のマスクを適用するようにします。



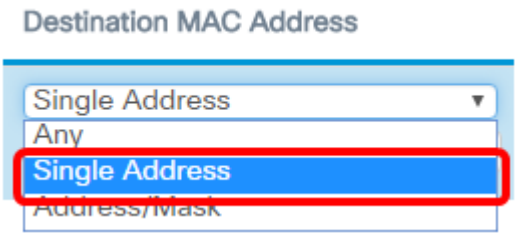
注: この例では、単一のアドレスは選択されます。

ステップ 14： *送信元MACアドレス* フィールドで送信元MACアドレスを入力して下さい。

注: この例では、10:60:4b:70:97:07 は入ります。 これは PC1 の MAC アドレスです。

ステップ 15： 宛先MAC アドレス ドロップダウン リストからの宛先MAC アドレスを定義して下さい。 オプションは次のとおりです:

- —このオプションは WAP があらゆる MAC アドレスからパケットにフィルタを適用するようにします。
- 単一のアドレス—このオプションは WAP が特定のMACアドレスからパケットにフィルタを適用するようにします。
- アドレス/マスク—このオプションは WAP が MAC アドレスにパケットにフィルタおよび WAP のマスクを適用するようにします。



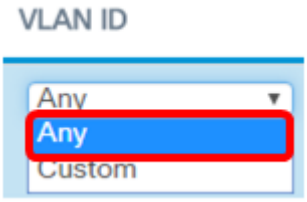
注: この例では、単一のアドレスは選択されます。

ステップ 16： **宛先MAC アドレス** フィールドで宛先MAC アドレスを入力して下さい。

注: この例では、28:f0:76:2a:21:92 は入ります。 これは Laptop2 の MAC アドレスです。

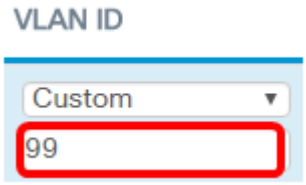
ステップ 17： ドロップダウン リストから VLAN ID を選択して下さい。

- —このオプションはネットワークによって VLAN ID を可能にします。
- カスタム—このオプションは仕様 VLAN ID を入力することを可能にします。 このオプションを選択する場合、ステップ 18 にスキップして下さい。



注: この例では、選択されます。

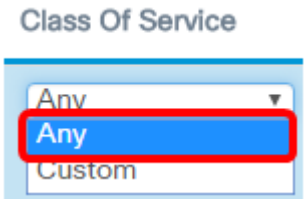
ステップ 18： 『Custom』 を選択 した場合（オプションの）、*VLAN ID フィールド*で VLAN ID を入力して下さい。



注: この例では、99 は入ります。

ステップ 19： （オプションの）ドロップダウン リストから a を Class of Service（CoS）選択して下さい。 オプションは次のとおりです:

- —このオプションはあらゆるプライオリティレベルとのパケットがネットワークに接続するようにします。
- カスタム—このオプションは特定のプライオリティレベルでパケットをフィルタリングすることを可能にします。



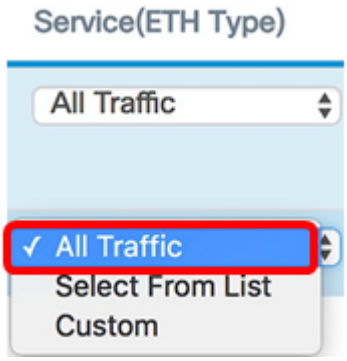
注: この例では、選択されます。 『Custom』 を選択 した場合、*Class of Service フィールド*で優先順位を入力して下さい。

ステップ 20： 割り当て＋ ルールを追加するためにボタンを再度クリックして下さい。

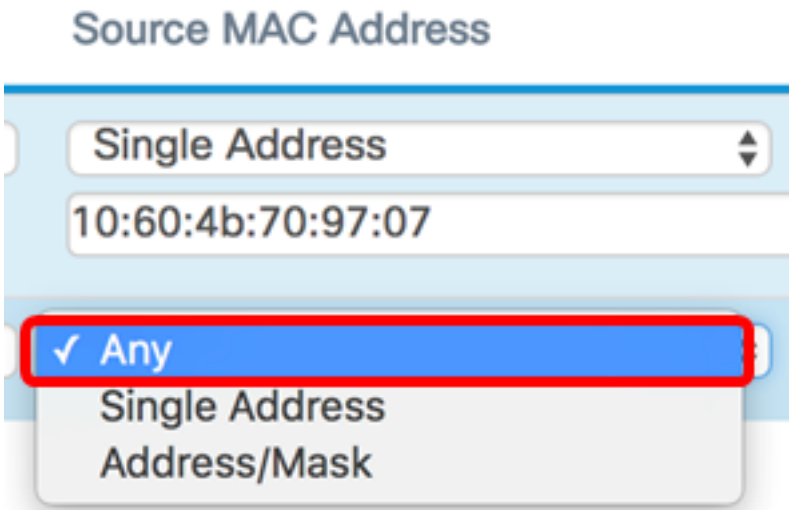
注: 暗黙の deny が作成される各ルールの終わりにあるのでネットワークのその他のデバイスからのトラフィックを許可する ACL に割り当てルールを追加することを強く推奨します。

ステップ 21： 処理ドロップダウン矢印をクリックし、**割り当てを**選択して下さい。

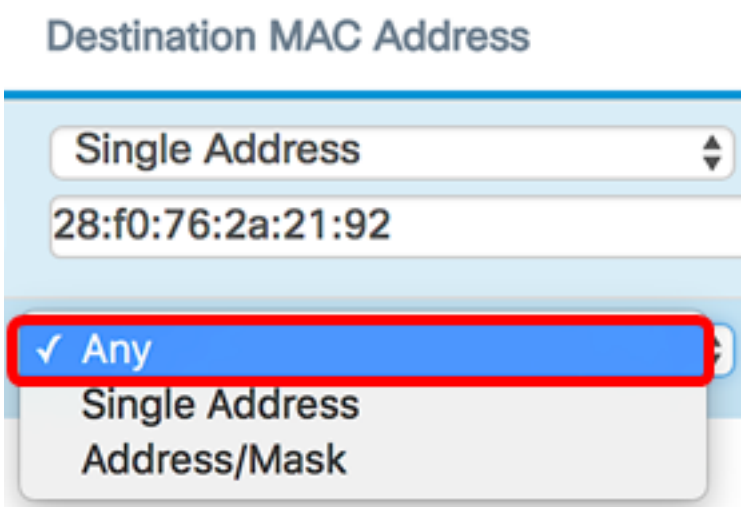
ステップ 22： サービス (ETH 型) ドロップダウン矢印をクリックし、**トラフィックを**『All』 を選択 して下さい。



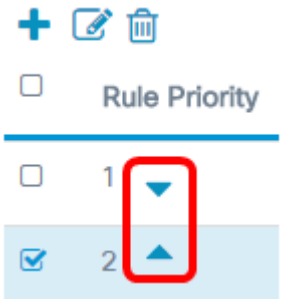
ステップ 23： 送信元MACアドレス ドロップダウン メニューをクリックし、選択して下さい。 これは最初のルールで示された PC1 MAC アドレスを除いてネットワークの他のどの MAC アドレスからのトラフィックも可能にします。



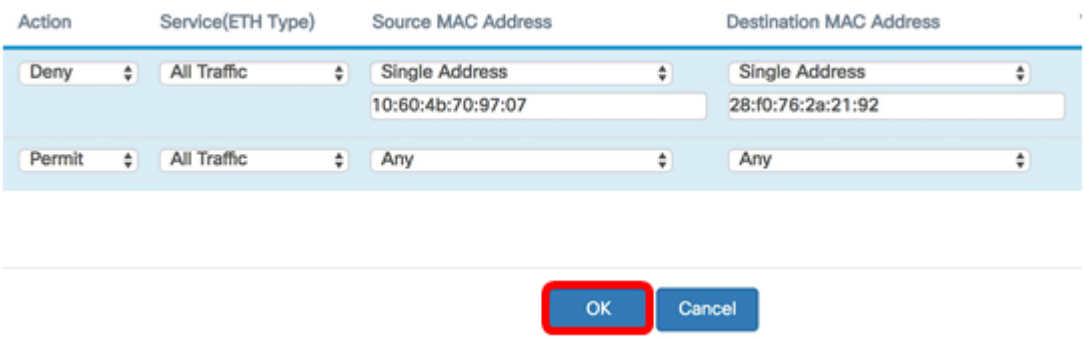
ステップ 24： 宛先MAC アドレス ドロップダウン メニューをクリックし、選択して下さい。 これはネットワークのあらゆる MAC アドレスに行くトラフィックを可能にします。



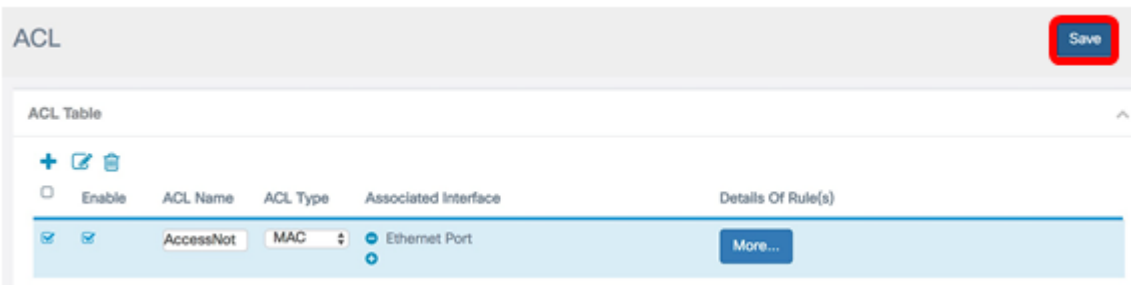
ステップ 25.(Optional) 上下矢印をクリックしてルールの優先順位を変更して下さいルールがきちんと整っているまで。



ステップ 26： [OK] をクリックします。



ステップ 27： [Save] をクリックします。



今 WAP125 か WAP581 アクセス ポイントの MAC ACL を設定する必要があります。

表示して下さいこの技術情報に関するビデオを...

Cisco からの他の Tech Talk を表示するためにここをクリックして下さい