WLC を使用したゲスト WLAN と内部 WLAN の設定例

目次

概要

このドキュメントでは、WLAN controller（WLC; WLAN コントローラ）と lightweight access point（LAP; Lightweight アクセス ポイント）を使用した、ゲスト用 wireless LAN（WLAN; ワイヤレス LAN）と安全な内部 WLAN の設定例を紹介しています。 このドキュメントの設定では、ゲスト WLAN ではユーザの認証に Web 認証を使用し、セキュアな内部 WLAN では Extensible Authentication Protocol（EAP）認証を使用しています。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- 基本的なパラメータによる WLC の設定方法に関する知識
- DHCP と Domain Name System（DNS; ドメイン ネーム システム）サーバの設定方法に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ファームウェア リリース 4.0 が稼働している Cisco 2006 WLC
- Cisco 1000 シリーズ LAP
- ファームウェア リリース 2.6 が稼働している Cisco 802.11a/b/g ワイヤレス クライアント アダプタ
- Cisco IOS® バージョン 12.4(2)XA を実行する Cisco 2811 ルータ
- Cisco IOS バージョン 12.0(5)WC3b が稼働している Cisco 3500 XL シリーズ スイッチ
- Microsoft Windows 2000 Server が稼働している DNS サーバ

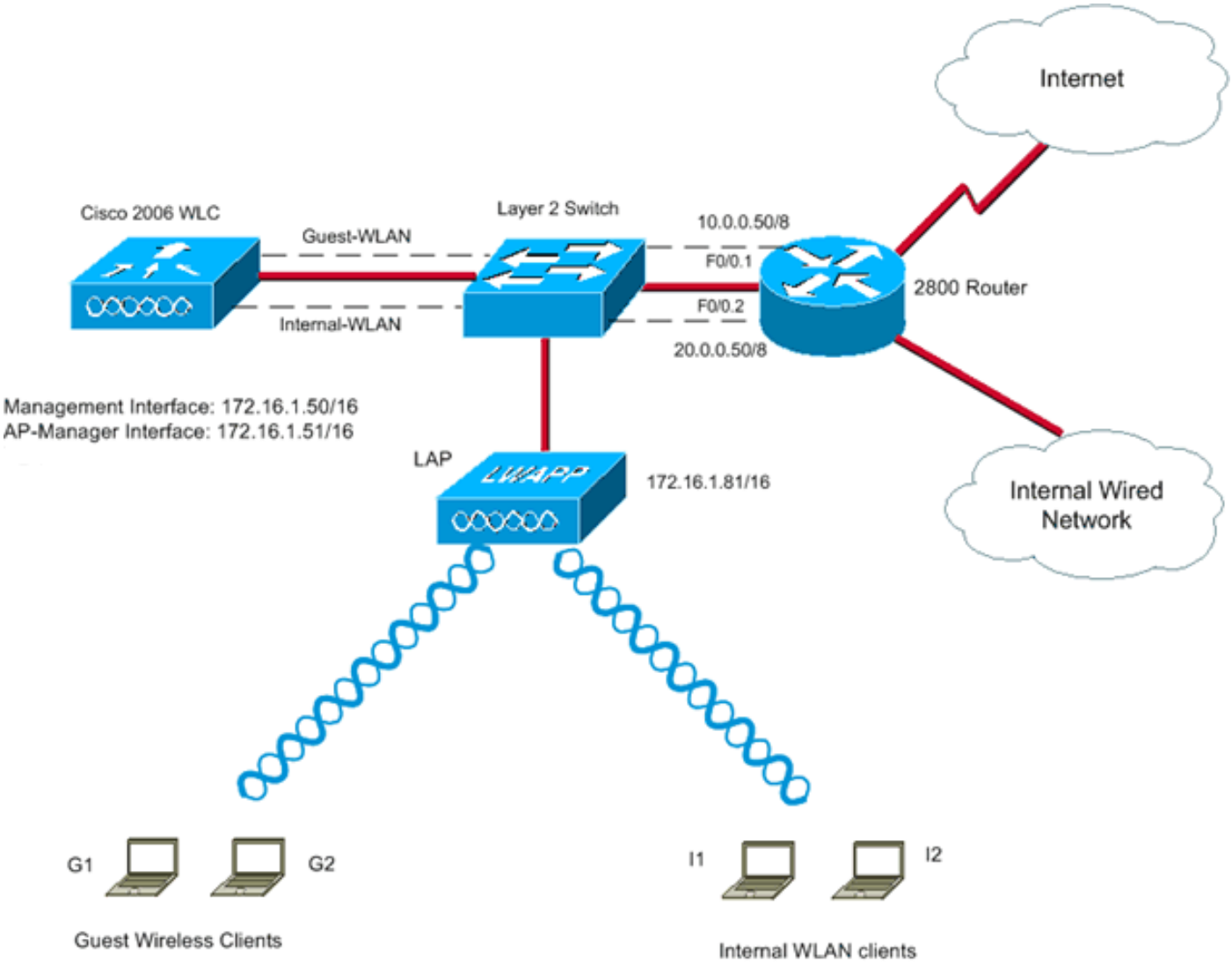
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ネットワーク構成

このドキュメントの設定例では、次のダイアグラムで示す構成を使用しています。 LAP は WLC に登録されています。 WLC はレイヤ 2 スイッチに接続されています。 ユーザを WAN に接続するルータもレイヤ 2 スイッチに接続されています。 WLAN を 2 つ作成する必要があります。1 つはゲスト ユーザ用で、もう 1 つは内部 LAN のユーザ用です。 また、ゲストおよび内部のワイヤレス クライアントに IP アドレスを提供するための DHCP サーバも必要です。 ゲスト ユーザはネットワークにアクセスするために Web 認証を使用します。 内部ユーザは EAP 認証を使用します。 2811 ルータはワイヤレス クライアント用の DHCP サーバとしても動作します。



注: このドキュメントでは、WLC は基本的なパラメータで設定されており、WLC に LAP が登録されていることを前提としています。 WLC での基本パラメータの設定と、LAP を WLC に登録する方法については、『ワイヤレス LAN コントローラ（WLC）への Lightweight AP（LAP）の登録』を参照してください。

一部のファイアウォールは、DHCP サーバとして登録した場合に、リレー エージェントからの DHCP 要求に対応しません。 WLC はクライアント用のリレー エージェントです。 DHCP サーバとして設定されたファイアウォールは、これらの要求を無視します。 クライアントは、直接ファイアウォールに接続されている必要があり、別のリレー エージェントやルータを経由して要求を送信することはできません。 ファイアウォールは、直接接続されている内部ホスト向けのシンプルな DHCP サーバとして動作することができます。 そのため、ファイアウォールは、直接接続されていて参照することのできる MAC アドレスによるテーブルを管理できます。 このような理由から、DHCP リレーからアドレスを割り当てようとしてもこのような処理は実行されず、パケットは廃棄されます。 PIX ファイアウォールにはこのような制約があります。

設定

このネットワーク構成用にデバイスを設定するには、次の手順を実行してください。

1. ゲスト ユーザおよび内部ユーザ向けの WLC でのダイナミック インターフェイスの設定
2. ゲスト ユーザおよび内部ユーザ向けの WLAN の作成
3. WLC にトランク ポートとして接続するレイヤ 2 スイッチ ポートの設定

4. 2 つの ▾WLAN▿ のためのルータの設定

ゲスト ユーザおよび内部ユーザ向けの WLC でのダイナミック インターフェイスの設定

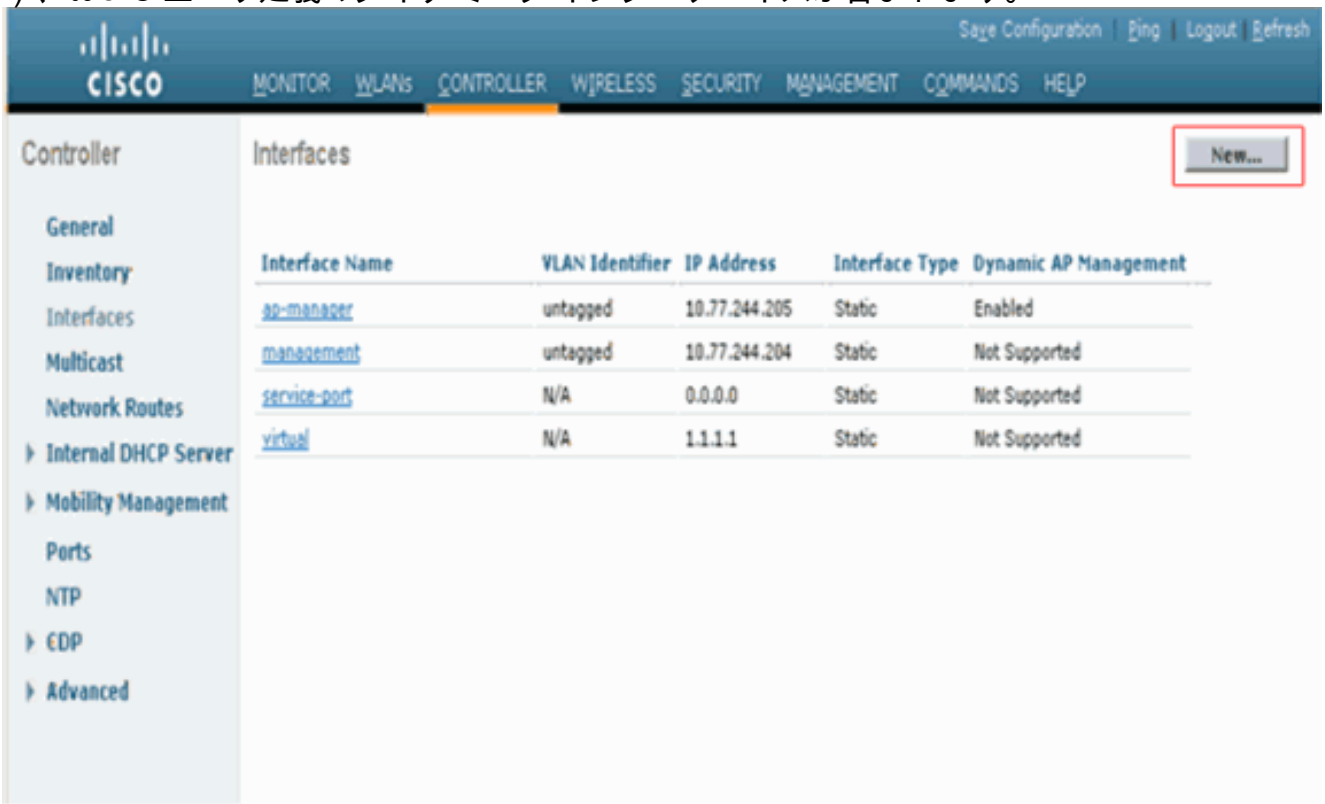
最初の手順は、WLC にダイナミック インターフェイスを 2 つ作成することです。1 つはゲスト ユーザ用で、もう 1 つは内部のユーザ用です。

このドキュメントの例では、ダイナミック インターフェイスに次のパラメータと値を使用します。

```
Guest-WLAN                                                    Internal-WLAN
VLAN Id : 10                                VLAN Id : 20
IP address: 10.0.0.10                             IP address: 20.0.0.10
Netmask: 255.0.0.0 Netmask: 255.0.0.0
Gateway: 10.0.0.50                              Gateway: 20.0.0.50
Physical port on WLC: 1                           Physical port on WLC: 1
DHCP server: 172.16.1.60                          DHCP server: 172.16.1.60
```

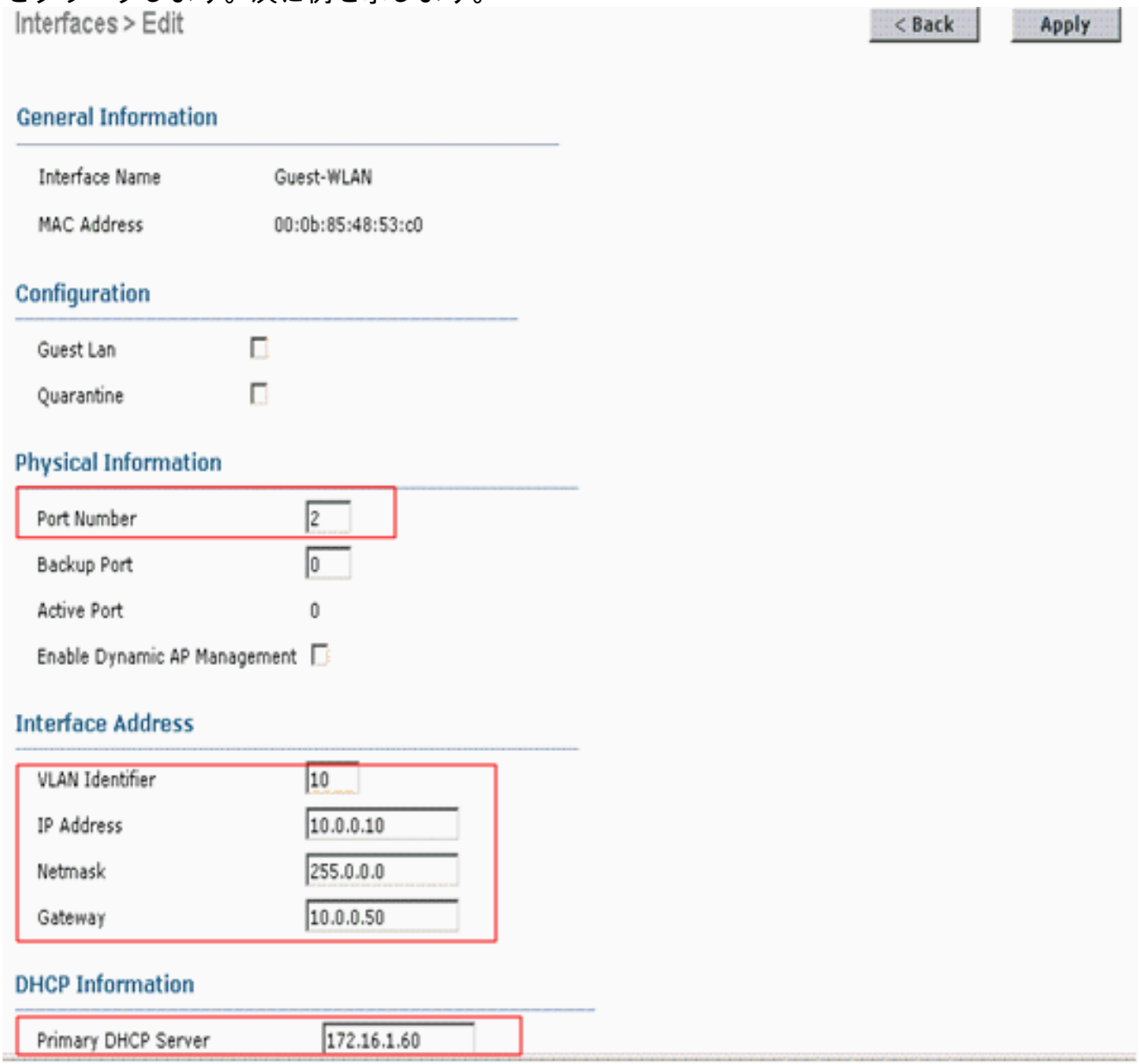
次の手順を実行します。

1. WLC GUI で、[Controllers] > [Interfaces] の順に選択します。[Interfaces] ウィンドウが表示されます。 このウィンドウには、コントローラに設定されているインターフェイスの一覧が表示されます。 これには、デフォルトのインターフェイス (管理インターフェイス、AP マネージャ インターフェイス、仮想インターフェイス、サービス ポート インターフェイス) 、およびユーザ定義のダイナミック インターフェイスが含まれます。



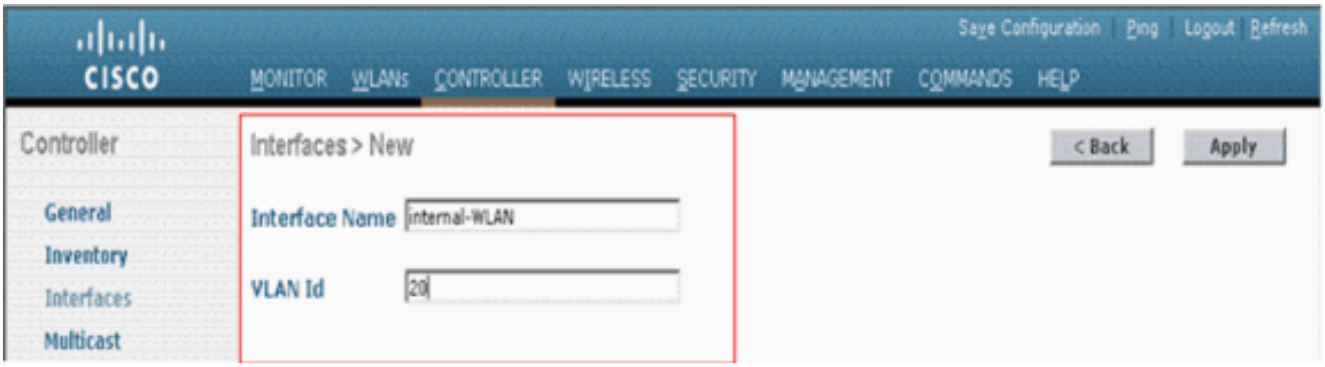
2. 新しいダイナミック インターフェイスを作成するには、[**New**] をクリックします。
3. [Interfaces > New] ウィンドウで、インターフェイス名と VLAN ID を入力します。 次に、[Apply] をクリックします。この例では、ダイナミック インターフェイスの名前に Guest-WLAN を指定し、VLAN ID に 10 を割り当てています。

4. [Interfaces > Edit] ウィンドウで、ダイナミック インターフェイスの IP アドレス、サブネット マスク、デフォルト ゲートウェイを入力します。 ダイナミック インターフェイスを WLC の物理ポートに割り当て、DHCP サーバの IP アドレスを入力します。 次に、[Apply] をクリックします。次に例を示します。

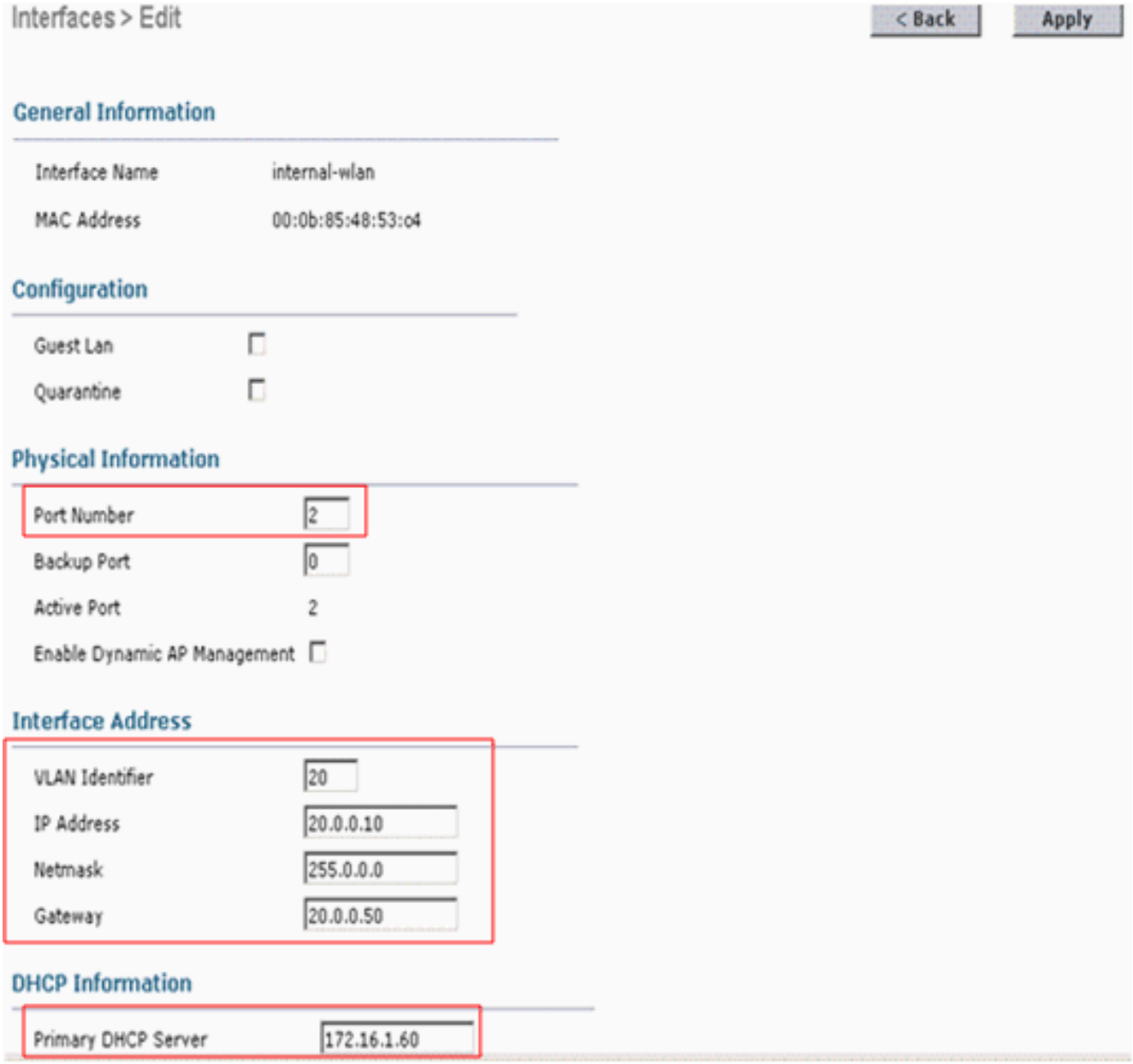


同じステップを実行して、内部 WLAN のダイナミック インターフェイスを作成します。

5. インターフェイス > New ウィンドウでは、内部ユーザ向けの動的インターフェイスのための内部 **WLAN を**入力し、VLAN ID のための **20 を**入力して下さい。 次に、[Apply] をクリックします。



6. [Interfaces > Edit] ウィンドウで、ダイナミック インターフェイスの IP アドレス、サブネット マスク、デフォルト ゲートウェイを入力します。 ダイナミック インターフェイスを WLC の物理ポートに割り当て、DHCP サーバの IP アドレスを入力します。 次に、[Apply] をクリックします。



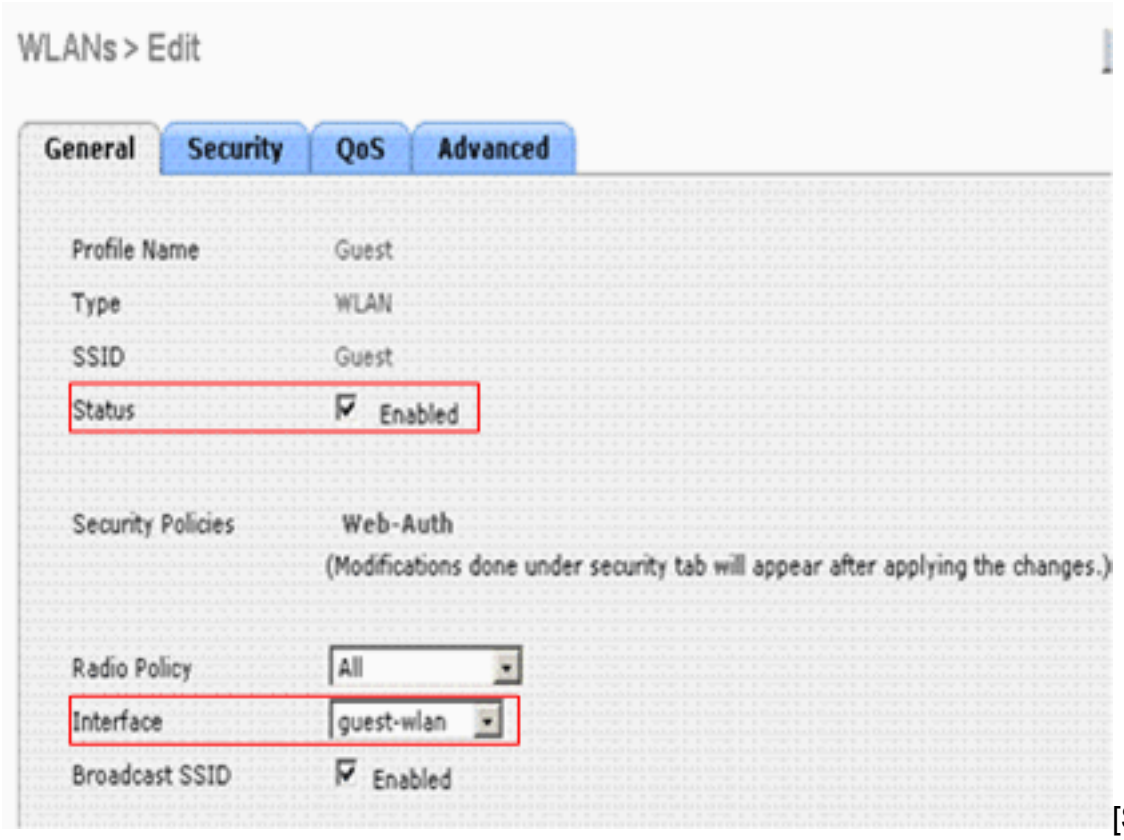
ここで、2 つのダイナミック インターフェイスが作成され、Interfaces ウィンドウに、コントローラに設定されたインターフェイスの一覧が次のように表示されます。

ゲスト ユーザおよび内部ユーザ向けの WLAN の作成

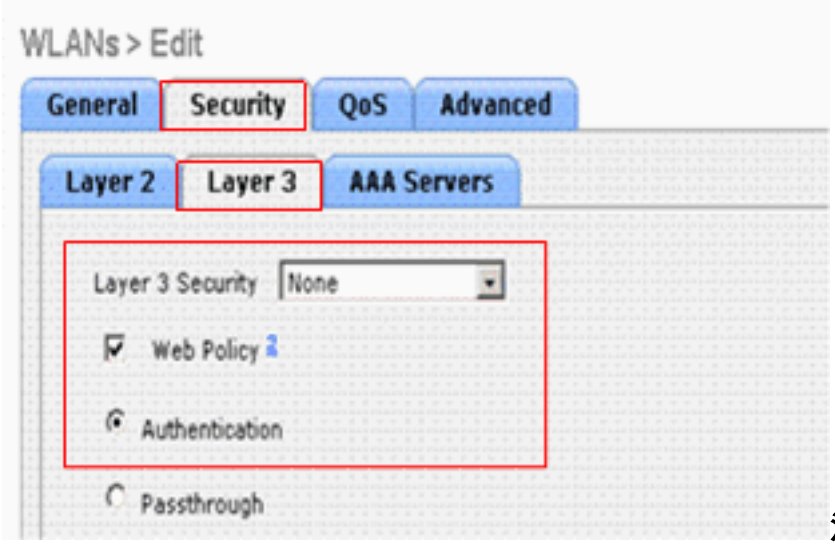
次の手順は、ゲスト ユーザ向けと内部ユーザ向けに WLAN を作成し、これらの WLAN にダイナミック インターフェイスをマップすることです。 また、ゲスト ユーザとワイヤレス ユーザを認証するために使用するセキュリティ方式を定義する必要があります。 次の手順を実行します。

1. WLAN を作成するために、コントローラの GUI で [WLANs] をクリックします。[WLANs] ウィンドウが表示されます。 このウィンドウには、コントローラに設定されている WLAN の一覧が表示されます。
2. 新しい WLAN を設定するために [New] をクリックします。この例では、WLAN に *Guest* という名前を付け、WLAN ID は 2 です。

3. 右上角にある **Apply** をクリックします。
4. WLAN > Edit 画面は現われます、さまざまなタブが含まれている。ゲスト用 WLAN の **General** タブで、Interface Name フィールドから **guest-wlan** を選択します。 これによって、先に作成したダイナミック インターフェイスの **guest-wlan** が WLAN **Guest** にマップされます。WLAN の Status が Enabled であることを確認します。



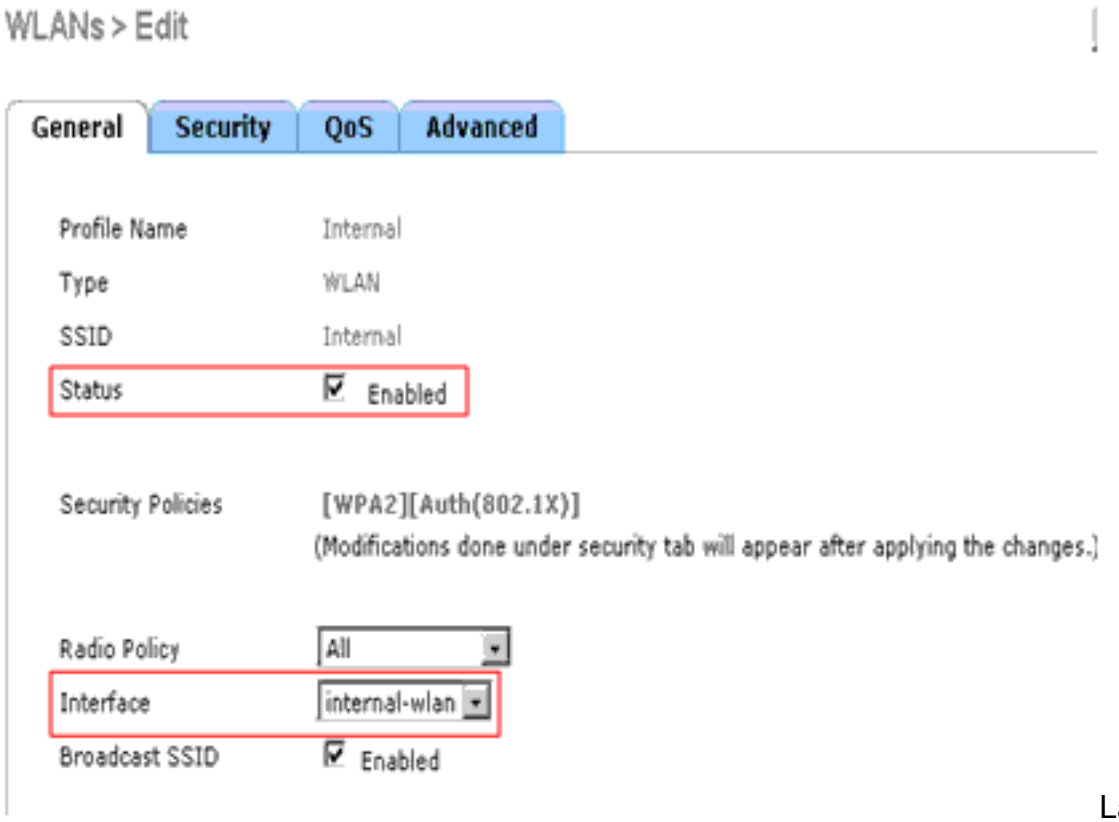
[Security] タブをクリックします。 この WLAN では、クライアントの認証にレイヤ 3 での Web 認証方式を使用します。 したがって、*Layer 3* Security のフィールドの下で、**None** を選択します。 *Layer 3* Security フィールドで、**Web Policy** ボックスにチェック マークを入れて、**Authentication** オプションを選択します。



注: Web 認証の詳細については、『ワイヤレス LAN コントローラの Web 認証の設定例』（英語）を参照してください。

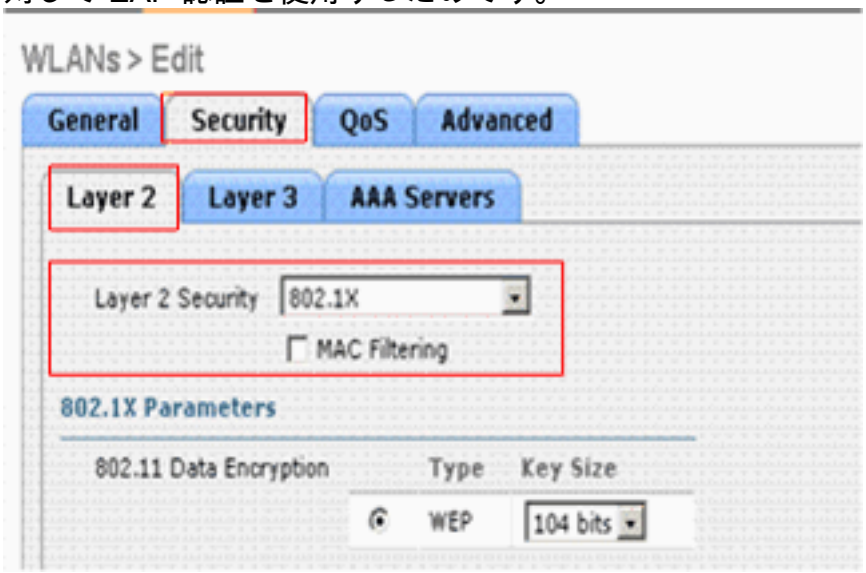
[Apply] をクリックします。

5. 内部ユーザ用の WLAN を作成します。 では WLAN > New ウィンドウは、**内部を**入力し、内部ユーザ向けの WLAN を作成するために『3』 を選択 します。 次に、[Apply] をクリックします。
6. WLANs > Edit ウィンドウが表示されます。 *General* タブで、Interface Name フィールドから **internal-wlan** を選択します。これによって、先に作成したダイナミック インターフェイスの **internal-wlan** が WLAN **Internal** にマップされます。 WLAN が Enabled であることを確認します。



Layer 2

Security オプションをデフォルト値の 802.1x のままにします。これは内部 WLAN ユーザに対して EAP 認証を使用するためです。

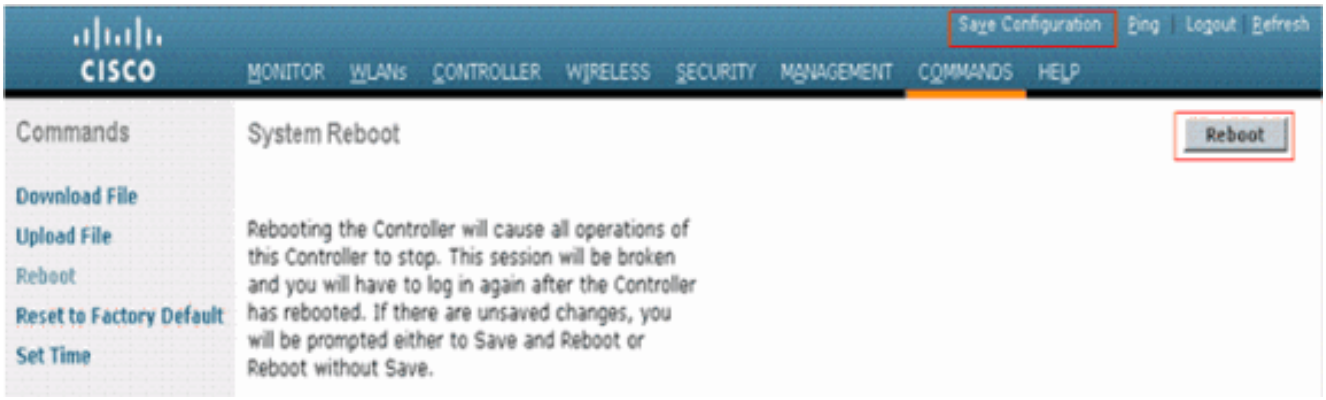


7. [Apply] をクリックします。WLAN ウィンドウが表示され、作成された WLAN のリストが表示されます。

注: WLC EAP WLAN [WLAN WLC EAP]

8. WLC の GUI で、**Save Configuration** をクリックし、続いてコントローラの GUI から

Commands をクリックします。 次に、Reboot オプションを選択して WLC をリブートし、Web 認証が有効になるようにします。



注: Save Configuration

WLC にトランク ポートとして接続するレイヤ 2 スイッチ ポートの設定

WLC に設定されている複数の VLAN サポートするように、スイッチ ポートを設定する必要があります。これは、WLC がレイヤ 2 スイッチに接続されているためです。 スイッチ ポートは 802.1Q トランク ポートとして設定する必要があります。

各コントローラ ポートの接続は 802.1Q トランクであり、隣接スイッチでもこのように設定する必要があります。 Cisco のスイッチでは、802.1Q トランクのネイティブ VLAN (たとえば **VLAN 1**) は、タグなしのままになっています。 したがって、コントローラのインターフェイスを隣接 Cisco スイッチのネイティブ VLAN を使用するよう設定する場合は、コントローラのインターフェイスをタグなしとして設定してください。

VLAN識別名用のゼロ値は (コントローラ > Interfaces ウィンドウで) 意味しますインターフェイスがタグが付いていないことを。 このドキュメントの例では、AP-Manager と Management Interfaces はデフォルトでタグなしの VLAN として設定されています。

コントローラのインターフェイスをゼロ以外の値に設定すると、スイッチのネイティブ VLAN にはタグ付けできなくなります。この VLAN はスイッチ上で許可される必要があります。 この例では、VLAN 60 がコントローラに接続されているスイッチ ポートのネイティブ VLAN として設定されています。

WLC に接続されているスイッチ ポートの設定を、次に示します。

```
interface f0/12
Description Connected to the WLC
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

これはトランク ポートとしてルータに接続しているスイッチ ポートの設定です。

```
interface f0/10
Description Connected to the Router
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

これは LAP に接続しているスイッチ ポートの設定です。 このポートはアクセス ポートとして設

定されています。

```
interface f0/9
Description Connected to the LAP
Switchport access vlan 60
switchport mode access
no ip address
```

2 つの WLAN のためのルータの設定

このドキュメントの例では、2811 ルータによってゲスト ユーザがインターネットに接続され、また内部の有線ユーザが内部のワイヤレス ユーザに接続されます。 また、ルータは DHCP サービスを提供するように設定する必要があります。

ルータでは、各 VLAN に対して、スイッチのトランク ポートに接続している FastEthernet インターフェイスの下に、サブ インターフェイスを作成します。 このサブ インターフェイスを対応する VLAN に割り当て、それぞれのサブネットから IP アドレスを設定します。

注: 設定全体ではなく、ルータの設定の中で関連のある部分だけを例示しています。

これは、この目的のためにルータで必要となる設定です。

ルータで DHCP サービスを設定するために発行する必要があるコマンドを、次に示します。

```
!
ip dhcp excluded-address 10.0.0.10
!--- IP excluded because this IP is assigned to the dynamic !--- interface created on the WLC.
ip dhcp excluded-address 10.0.0.50 !--- IP excluded because this IP is assigned to the !--- sub-interface on the router. ip dhcp excluded-address 20.0.0.10 !--- IP excluded because this IP is assigned to the dynamic !--- interface created on the WLC. ip dhcp excluded-address 20.0.0.50 !--- IP excluded because this IP is assigned to the sub-interface on the router. ! ip dhcp pool Guest !--- Creates a DHCP pool for the guest users. network 10.0.0.0 255.0.0.0 default-router 10.0.0.50 dns-server 172.16.1.1 !--- Defines the DNS server. ! ip dhcp pool Internal network 20.0.0.0 255.0.0.0 default-router 20.0.0.50 !--- Creates a DHCP pool for the internal users. !
```

次のコマンドは、設定例の FastEthernet インターフェイスに対して発行する必要があります。

```
!
interface FastEthernet0/0
 description Connected to L2 Switch
 ip address 172.16.1.60 255.255.0.0
 duplex auto
 speed auto
!--- Interface connected to the Layer 2 switch. ! interface FastEthernet0/0.1 description Guest VLAN encapsulation dot1Q 10 ip address 10.0.0.50 255.0.0.0 !--- Creates a sub-interface under FastEthernet0/0 for the guest VLAN. ! interface FastEthernet0/0.2 description Internal VLAN encapsulation dot1Q 20 ip address 20.0.0.50 255.0.0.0 !--- Creates a sub-interface under FastEthernet0/0 for the internal VLAN. !
```

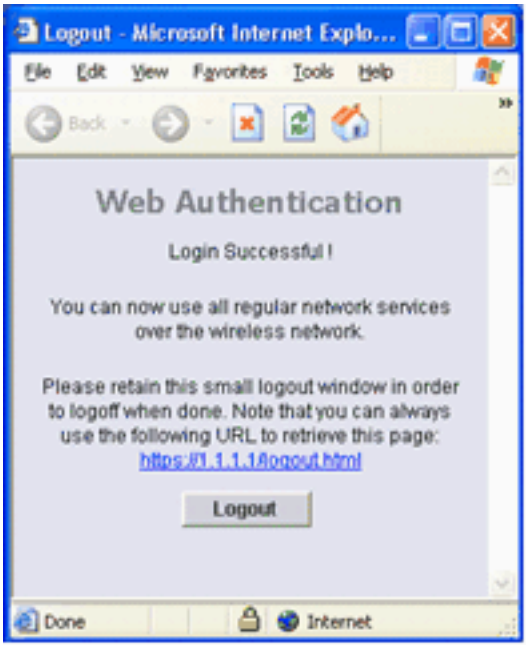
確認

ここでは、設定が正常に動作していることを確認します。

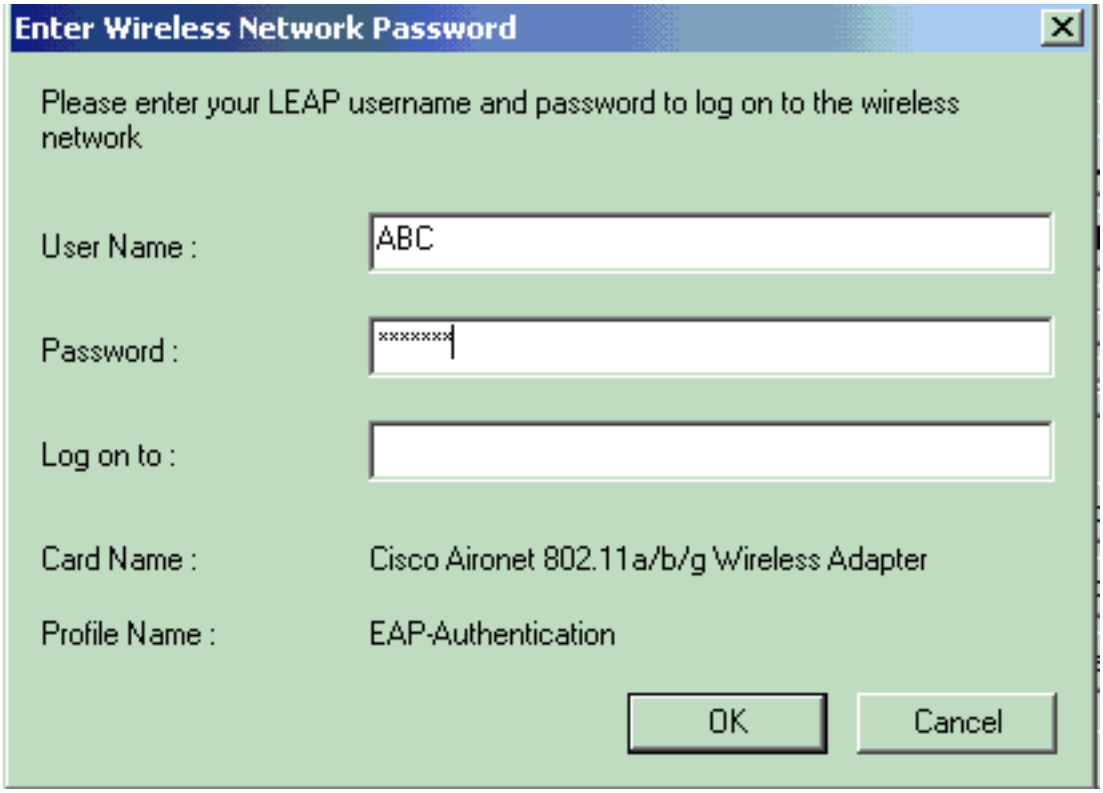
設定が意図したとおりに動作していることを確認するために、2 つのワイヤレス クライアントを接続します。1 つはゲスト ユーザ（service set identifier（SSID）は **Guest**）、もう 1 つは内部ユーザ（SSID は **Internal**）です。

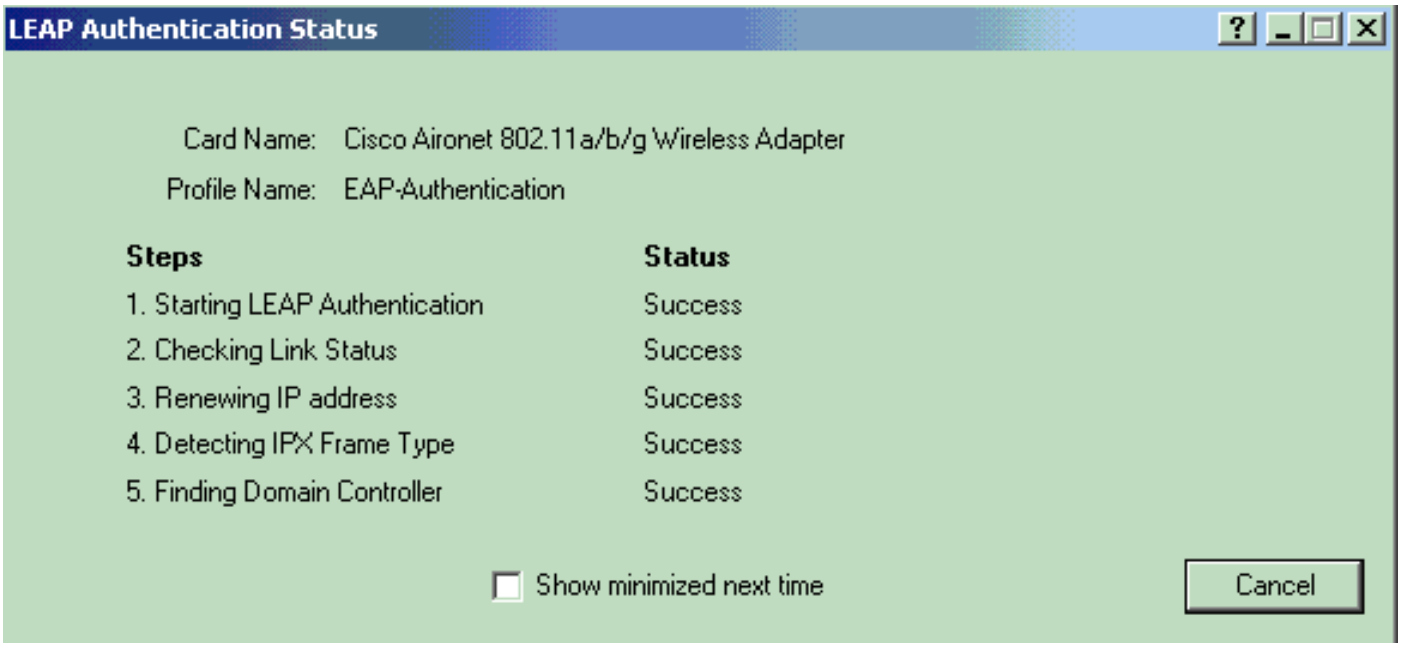
ゲスト WLAN は Web 認証を使用するよう設定されていることに注意してください。 ゲスト ワ

イヤレス クライアントが起動したら、Web ブラウザに任意の URL を入力します。 デフォルトの Web 認証ページがポップアップ表示され、ユーザ名とパスワードを入力するように求められます。 ゲスト ユーザが有効なユーザ名とパスワードを入力すると、WLC によってゲスト ユーザが認証され、ネットワーク（あるいはインターネット）へのアクセスが許可されます。 ユーザに表示される Web 認証のウィンドウと、認証が正しく行われた場合の画面の例を次に示します。



この例の内部 WLAN は、802.1x 認証を使用するように設定されています。 内部 WLAN クライアントが起動すると、クライアントでは EAP 認証が使用されます。 EAP 認証用にクライアントを設定する方法についての詳細は、『Cisco Aironet 802.11a/b/g ワイヤレス LAN クライアント アダプタ（CB21AG および PI21AG）インストレーション コンフィギュレーション ガイド』の「EAP 認証の使用方法」のセクションを参照してください。 認証が正しく行われると、ユーザは内部ネットワークにアクセスできるようになります。 この例では、Lightweight Extensible Authentication Protocol（LEAP）認証を使用する内部ワイヤレス クライアントを示しています。





トラブルシューティング

トラブルシューティング手順

ここでは、設定に関するトラブルシューティングについて説明します。

設定が意図したとおりに動作しない場合は、次の手順を実行してください。

1. WLC に設定されているすべての VLAN が、WLC に接続されているスイッチ ポートで許可されていることを確認します。
2. WLC とルータに接続してされているスイッチ ポートがトランク ポートとして設定されていることを確認します。

3. 使用している VLAN ID が WLC とルータで同じであることを確認します。
4. クライアントが DHCP サーバから DHCP アドレスを受け取っているかどうかを確認します。 受け取っていない場合は、DHCP サーバが正しく設定されているかどうかを確認します。 クライアントの問題のトラブルシューティングについての詳細は、『Cisco Unified Wireless Network でのクライアントの問題のトラブルシューティング』を参照してください。

Web 認証でよく生じる問題の 1 つは、Web 認証ページへのリダイレクトが動作しないというものです。 ブラウザを開いても、Web 認証ウィンドウが表示されません。 この場合は、**https://1.1.1.1/login.html** と手動で入力し、Web 認証ウィンドウを表示する必要があります。 これは、Web 認証ページへのリダイレクトが発生する前に動作する必要のある DNS ルックアップで行う必要があります。 ワイヤレス クライアントでブラウザのホームページがドメイン名を指している場合は、リダイレクトが動作するためには、クライアントが関連付けられた後で、nslookup を正常に実行する必要があります。

また、3.2.150.10 よりも前のバージョンが稼働する WLC の場合の Web 認証では、その SSID でユーザがインターネットへのアクセスを試みると、コントローラの管理インターフェイスが DNS クエリーを行い、URL が有効かどうかを確認します。 有効な場合は、その URL で仮想インターフェイスの IP アドレスによって認証ページが表示されます。 ユーザがログインに成功すると、元の要求をクライアントに送り返すことが許可されます。 これは、Cisco Bug ID CSCsc68105（登録ユーザ専用）によるものです。 詳細については、ワイヤレス LAN コントローラ（WLC）のトラブルシューティング Web 認証を参照して下さい。

トラブルシューティングのためのコマンド

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

次の debug コマンドを使用して、設定のトラブルシューティングを行うことができます。

- **debug mac addr <client-MAC-address xx: xx: xx: xx: xx: xx>**：クライアントの MAC アドレスのデバッグを設定します。
- **debug aaa all enable**：すべての AAA メッセージのデバッグを設定します。
- **debug pem state enable**：Policy Manager ステート マシンのデバッグを設定します。
- **debug pem events enable**：ポリシー マネージャ イベントのデバッグを設定します。
- **debug dhcp message enable** — DHCP クライアント アクティビティについてのデバッグ情報を表示する、DHCP パケットのステータスを監視するためにこのコマンドを使用して下さい。
- **debug dhcp packet enable**：DHCP パケット レベル情報を表示するには、このコマンドを使用します。
- **debug pm ssh-appgw enable**：アプリケーション ゲートウェイのデバッグを設定します。
- **debug pm ssh-tcp enable**：ポリシー マネージャ tcp 処理のデバッグを設定します。

これらの **debug** コマンドの一部のサンプル出力を次に示します。

注: スペースの制約により 2 行に渡って表示されている行もあります。

```
(Cisco Controller) >debug dhcp message enable Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp
option len, including the magic cookie = 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp
option: received DHCP REQUEST msg Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option:
skipping option 61, len 7 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: requested ip =
10.0.0.1 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 12, len 3 Fri
Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 7 Fri Mar 2 16:01:43
```

2007: 00:40:96:ac:e6:57 dhcp option: vendor class id = MSFT5.0 (len 8) Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 55, len 11 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 Forwarding DHCP packet (332 octets)from 00:40:96:ac:e6:57 -- packet received on direct-connect port requires forwarding to external DHCP server. Next-hop is 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option len, including the magic cookie = 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: received DHCP ACK msg Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: server id = 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: lease time (seconds) =86400 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 58, len 4 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 59, len 4 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 6 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: netmask = 255.0.0.0 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: gateway = 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64

(Cisco Controller) >debug dhcp packet enable Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet: Client 00:40:96:ac:e6:57 DHCP Op: BOOTREQUEST(1), IP len: 300, switchport: 1, encap: 0xec03 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: dhcp request, client: 00:40:96:ac:e6:57: dhcp op: 1, port: 2, encap 0xec03, old mscb port number: 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Determing relay for 00:40:96:ac:e6:57 dhcpServer: 10.0.0.50, dhcpNetmask: 255.0.0.0, dhcpGateway: 10.0.0.50, dhcpRelay: 10.0.0.10 VLAN: 30 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Relay settings for 00:40:96:ac:e6:57 Local Address: 10.0.0.10, DHCP Server: 10.0.0.50, Gateway Addr: 10.0.0.50, VLAN: 30, port: 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP REQUEST msg Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 op: BOOTREQUEST, htype: Ethernet,hlen: 6, hops: 1 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr: 0.0.0.0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 10.0.0.10 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP request to 10.0.0.50, len 350,switchport 2, vlan 30 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet: Client 00:40:96:ac:e6:57 DHCP Op: BOOTREPLY(2), IP len: 300, switchport: 2, encap: 0xec00 Fri Mar 2 16:06:35 2007: DHCP Reply to AP client: 00:40:96:ac:e6:57, frame len412, switchport 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP ACK msg Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr: 10.0.0.1 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 0.0.0.0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 server id: 1.1.1.1 rcvd server id: 10.0.0.50

(Cisco Controller) >debug aaa all enable Fri Mar 2 16:22:40 2007: **User user1 authenticated** Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 **Returning AAA Error 'Success' (0) for mobile 00:40:96:ac:e6:57** Fri Mar 2 16:22:40 2007: AuthorizationResponse: 0xbadff97c Fri Mar 2 16:22:40 2007: structureSize.....70 Fri Mar 2 16:22:40 2007: resultCode.....0 Fri Mar 2 16:22:40 2007: protocolUsed.....0x00000008 Fri Mar 2 16:22:40 2007: proxyState.....00:40:96:AC:E6:57-00:00 Fri Mar 2 16:22:40 2007: Packet contains 2 AVPs: Fri Mar 2 16:22:40 2007: AVP[01] Service-Type.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[02] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Applying new AAA override for station 00:40:96:ac:e6:57 Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57 source: 48, valid bits: 0x1 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Unable to apply override policy for station 00:40:96:ac:e6:57 - VapAllowRadiusOverride is FALSE Fri Mar 2 16:22:40 2007: AccountingMessage Accounting Start: 0xa62700c Fri Mar 2 16:22:40 2007: Packet contains 13 AVPs: Fri Mar 2 16:22:40 2007: AVP[01] User-Name.....user1 (5 bytes) Fri Mar 2 16:22:40 2007: AVP[02] Nas-Port.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[03] Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[04] NAS-Identifier.....0x574c4331 (1464615729) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[05] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[06] Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes) Fri Mar 2 16:22:40 2007: AVP[07] Acct-Authentic.....0x00000002 (2) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[08] Tunnel-Type.....0x0000000d (13) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[09] Tunnel-Medium-Type.....0x00000006 (6) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[10] Tunnel-Group-Id.....0x3330 (13104) (2 bytes) Fri Mar 2 16:22:40 2007: AVP[11] Acct-Status-Type.....0x00000001 (1)

(4 bytes) Fri Mar 2 16:22:40 2007: AVP[12] Calling-Station-Id.....10.0.0.1 (8 bytes) Fri Mar 2 16:22:40 2007: AVP[13] Called-Station-Id.....10.77.244.210 (13 bytes) when web authentication is closed by user: (Cisco Controller) >Fri Mar 2 16:25:47 2007: AccountingMessage Accounting Stop: 0xa627c78 Fri Mar 2 16:25:47 2007: Packet contains 20 AVPs: Fri Mar 2 16:25:47 2007: AVP[01] User-Name.....user1 (5 bytes) Fri Mar 2 16:25:47 2007: AVP[02] Nas-Port.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[03] Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[04] NAS-Identifier.....0x574c4331 (1464615729) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[05] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[06] Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes) Fri Mar 2 16:25:47 2007: AVP[07] Acct-Authentic.....0x00000002 (2) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[08] Tunnel-Type.....0x0000000d (13) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[09] Tunnel-Medium-Type.....0x00000006 (6) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[10] Tunnel-Group-Id.....0x3330 (13104) (2 bytes) Fri Mar 2 16:25:47 2007: AVP[11] Acct-Status-Type.....0x00000002 (2) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[12] Acct-Input-Octets.....0x0001820e (98830) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[13] Acct-Output-Octets.....0x00005206 (20998) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[14] Acct-Input-Packets.....0x000006ee (1774) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[15] Acct-Output-Packets.....0x00000041 (65) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[16] Acct-Terminate-Cause.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[17] Acct-Session-Time.....0x000000bb (187) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[18] Acct-Delay-Time.....0x00000000 (0) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[19] Calling-Station-Id.....10.0.0.1 (8 bytes) Fri Mar 2 16:25:47 2007: AVP[20] Called-Station-Id.....10.77.244.210 (13 bytes)
(Cisco Controller) >debug pem state enable Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 **WEBAUTH_REQD (8) Change state to START (0)** Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 **AUTHCHECK (2) Change stateto L2AUTHCOMPLETE (4)** Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4) Change state to WEBAUTH_REQD (8) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14) Fri Mar 2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_NOL3SEC (14) Change state to RUN (20) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:25 2007: 00:40:96:af:a3:40 40.0.0.1 DHCP_REQD (7) Change stateto RUN (20) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:34 2007: 00:16:6f:6e:36:2b 30.0.0.2 DHCP_REQD (7) Change stateto WEBAUTH_REQD (8)
(Cisco Controller) >debug pem events enable Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Initializing policy Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:5b:fb:d0 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Adding TMP rule Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Replacing Fast Path rule type = Temporary Entry on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL ID 255) Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Deleting mobile policy rule 27 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 Adding Web RuleID 28 for mobile 00:40:96:ac:e6:57 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Adding TMP rule Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) ReplacingFast Path rule type = Temporary Entry on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL ID 255) Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Removed NPU entry. Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU

entry of type 8

関連情報

- ワイヤレス ゲスト アクセス FAQ
- Cisco WLAN Controller を使用した有線ゲスト アクセスの設定例
- ワイヤレス LAN コントローラでの認証の設定例
- ワイヤレス LAN コントローラを使用した外部 Web 認証の設定例
- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 4.0
- ワイヤレス製品に関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems