ワイヤレス LAN コントローラ（WLC）上の Web 認証のトラブルシューティング

目次

概要

このドキュメントは、WLC 環境の Web 認証問題のトラブルシューティングに役立つヒントについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Lightweight Access Point Protocol（LWAPP）/Control And Provisioning of Wireless Access Points（CAPWAP）に関する知識。
- 基本動作用の Lightweight Access Point（LAP）および WLC の設定に関する知識。
- Web 認証および WLC での Web 認証の設定に関する基本的な知識。 WLC に Web 認証を設定する詳細については、「ワイヤレス LAN コントローラの Web 認証の設定例」を参照してください。

使用するコンポーネント

このドキュメントの情報は、ファームウェア バージョン 7.0.98.0 が稼働する WLC 5500 に基づくものです。

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。

関連製品

このドキュメントは、次のハードウェアにも使用できます。

- Cisco 5500 シリーズ ワイヤレス コントローラ
- Cisco 4400 シリーズ ワイヤレス LAN コントローラ
- Cisco 4100 シリーズ ワイヤレス LAN コントローラ
- Cisco 2500 シリーズ ワイヤレス コントローラ
- Cisco 2100 シリーズ ワイヤレス LAN コントローラ
- Cisco 2000 シリーズ ワイヤレス LAN コントローラ
- Cisco Airespace 3500 シリーズ WLAN コントローラ
- Cisco Airespace 4000 シリーズ ワイヤレス LAN コントローラ
- Cisco ワイヤレス LAN コントローラ モジュール
- Cisco Catalyst 6500 シリーズ ワイヤレス サービス モジュール（WiSM）
- Cisco Flex 7500 シリーズ ワイヤレス コントローラ
- Cisco Wireless Services Module 2（WiSM2）
- Cisco Catalyst 3750 シリーズ統合型ワイヤレス LAN コントローラ

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。

WLC での Web 認証

Web 認証とは、事前認証 Access Control List（ACL; アクセス コントロール リスト）で許可されたトラフィックを除いて、有効なユーザ名とパスワードが正しく入力されるまで特定のクライアントからの IP トラフィック（DHCP 関連のパケット/DNS 関連のパケットは除く）をコントローラで許可しないようにするレイヤ 3 セキュリティ機能です。 Web 認証は、認証の前にクライアントが IP アドレスを取得することを許可する唯一のセキュリティ ポリシーです。 これは、サプリカントやクライアント ユーティリティを必要としない簡単な認証方式です。Web 認証は WLC 上でローカルに実行することも、RADIUS サーバ経由で実行することもできます。 一般に、Web 認証はゲスト アクセス ネットワークを展開する場合に使用されます。

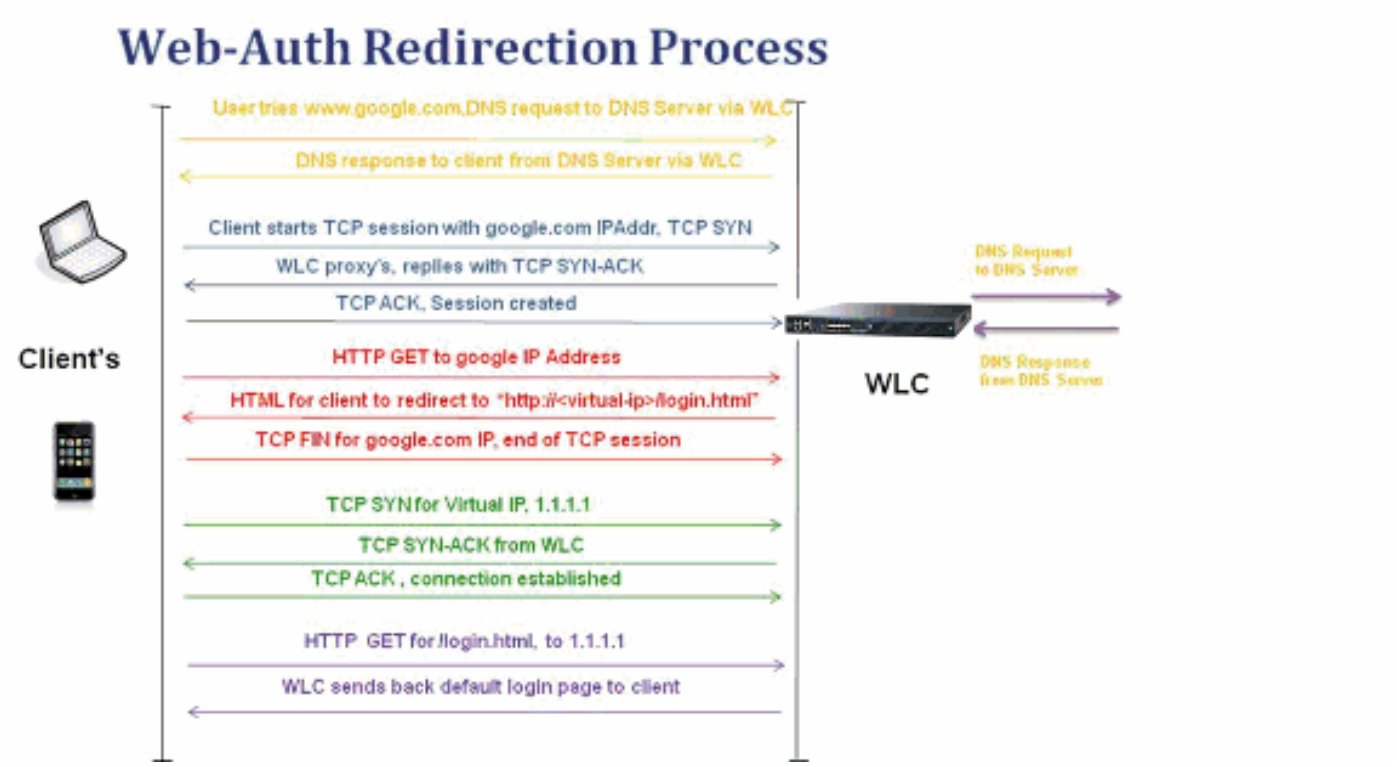
Web 認証は、クライアントからの最初の TCP HTTP（ポート 80）GET パケットをコントローラがインターセプトしたときに開始されます。 クライアントの Web ブラウザがそこまで到達するには、クライアントがまず IP アドレスを取得し、Web ブラウザのために URL の IP アドレスへの変換（DNS 解決）を行う必要があります。 これによって、Web ブラウザが HTTP GET を送信する IP アドレスを認識できます。

WLAN で Web 認証が設定されている場合、コントローラは認証プロセスが完了するまで、クライアントからの DHCP および DNS トラフィックを除くすべてのトラフィックをブロックします。 クライアントが最初の HTTP GET を TCP ポート 80 に送信したとき、コントローラは処理のためにそのクライアントを https:1.1.1.1/login.html にリダイレクトします。 このプロセスは最終的にログイン Web ページを起動します。

注: Web 認証に外部 Web サーバを使用する場合、一部の WLC プラットフォームには外部 Web サーバ用の事前認証 ACL（Cisco 5500 シリーズ コントローラ、Cisco 2100 シリーズ コントローラ、Cisco 2000 シリーズ、およびコントローラ ネットワーク モジュールが含まれる ACL）が必要になります。 他の WLC プラットフォームには、事前認証 ACL は必須ではありません。

注: ただし、外部 Web 認証を使用する場合は、外部 Web サーバ用の事前認証 ACL を設定することを推奨します。

このセクションでは、Web 認証のリダイレクトの手順を詳しく説明します。

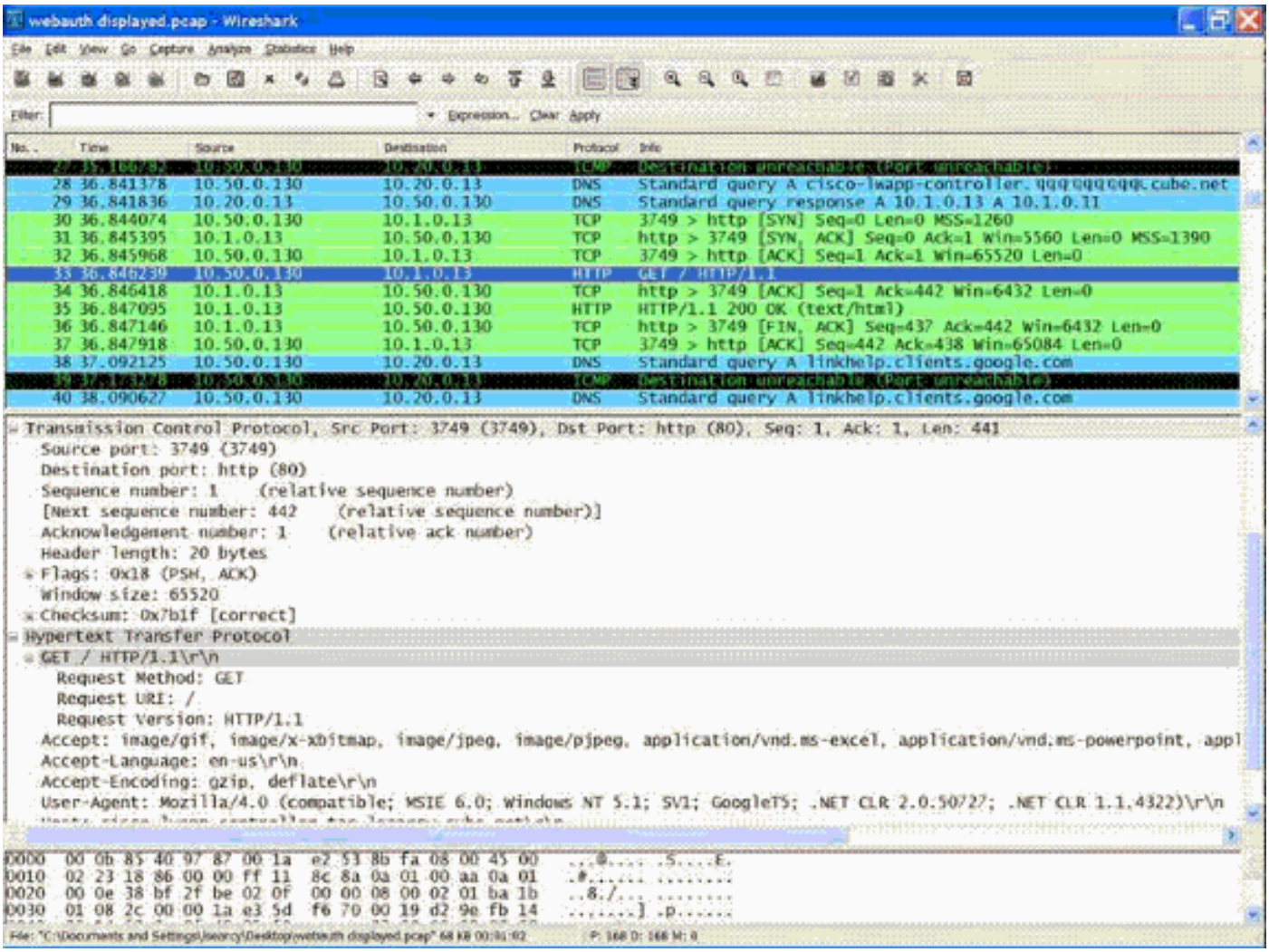


- Web ブラウザを開き、たとえば、http://www.google.com などの URL を入力します。 クライアントは、宛先の IP を取得するため、この URL の DNS 要求を送信します。 WLC が DNS サーバに DNS 要求をバイパスし、DNS サーバが宛先 www.google.com の IP アドレスを含む DNS 応答を返します。この応答はワイヤレス クライアントに転送されます。
- 続いて、クライアントは宛先 IP アドレスを使用して TCP 接続を開始しようとします。 Www.google.com の IP アドレスを宛先とする TCP SYN パケットが送信されます。
- WLC にはクライアント用に設定されたルールがあるため、www.google.com のプロキシとして機能します。 WLC は、www.google.com の IP アドレスを送信元とする TCP SYN-ACK パケットをクライアントに戻します。 クライアントは、3 ウェイ TCP ハンドシェイクを完了するために、TCP ACK パケットを返し、TCP 接続が完全に確立されます。
- クライアントは、www.google.com 宛ての HTTP GET パケットを送信します。 WLC はこのパケットをインターセプトし、リダイレクト処理のために送信します。 HTTP アプリケーション ゲートウェイは、HTML 本文を準備し、クライアントから要求された HTTP GET への応答として返します。 この HTML により、クライアントは WLC のデフォルト Web ページの URL (たとえば、http://<Virtual-Server-IP>/login.html.) に転送されます。
- クライアントは、たとえば www.google.com などの IP アドレスとの TCP 接続を閉じます。
- 次に、クライアントは http://1.1.1.1/login.html に移動するために、WLC の仮想 IP アドレスで TCP 接続を開こうとします。 WLC へ 1.1.1.1 に対する TCP SYN パケットを送信します。
- WLC は、TCP SYN-ACK で応答し、クライアントは WLC に TCP ACK を返して、ハンドシェイクが完了します。
- クライアントは、ログイン ページを要求するために、1.1.1.1 を宛先とする、/login.html の HTTP GET を送信します。
- この要求は、WLC の Web サーバに到達して許可され、サーバはデフォルト ログイン ページで応答します。 クライアントは、ブラウザ ウィンドウでログイン ページを受信し、ユーザはブラウザでログインできます。

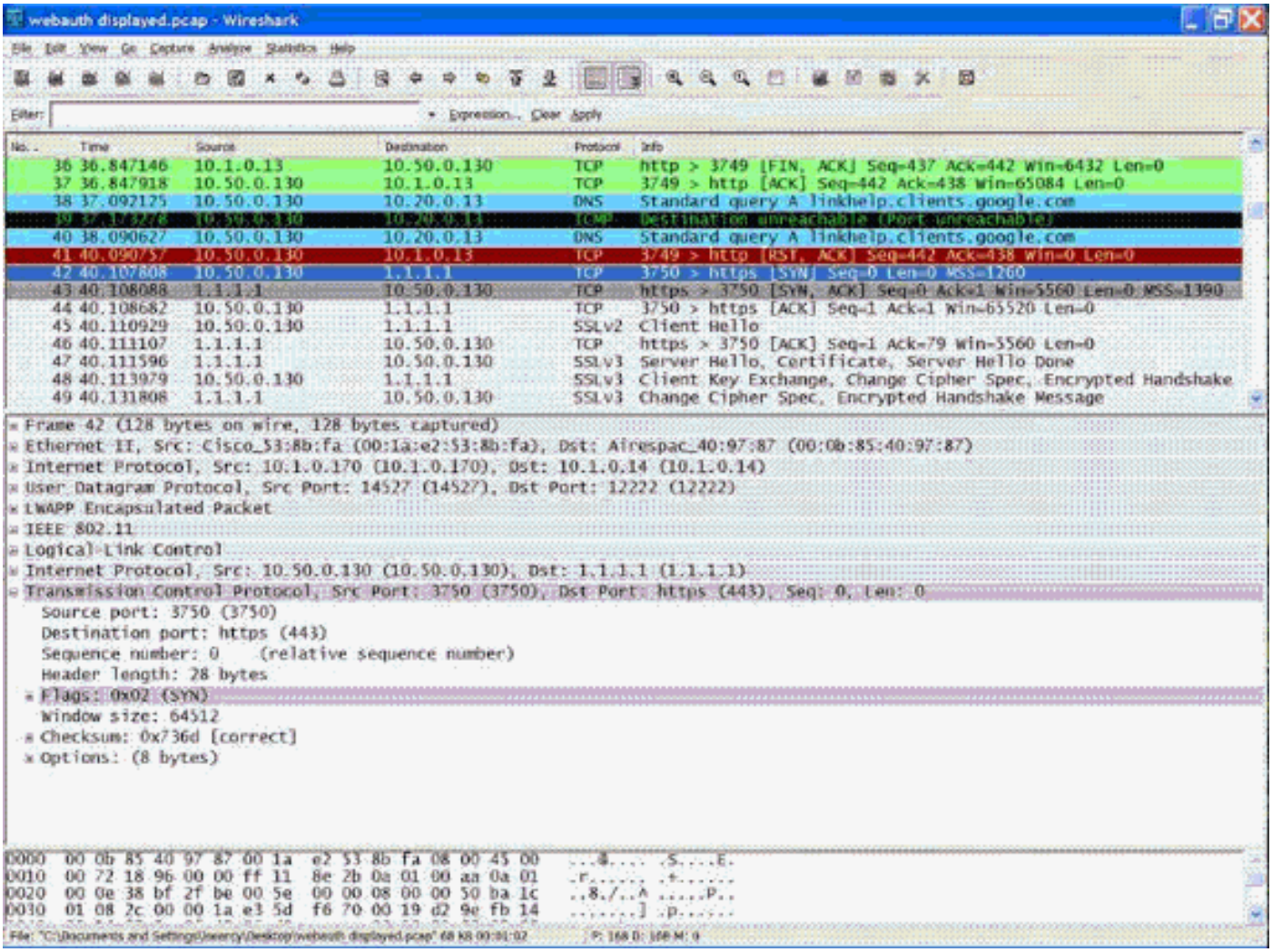
次に例を示します。 この例では、クライアントの IP アドレスは 10.50.0.130 です。 クライアントは、10.1.0.13 にアクセスしていた Web サーバへの URL を解決しました。 例からわかるように、クライアントは、3 ウェイ ハンドシェイクを行って、TCP 接続を開始し、パケット 30 で始まる HTTP GET を送信しました。 コントローラは、パケットをインターセプトし、コード 200 で応答しています。 コード 200 のパケットには、次のように、リダイレクト URL が含まれています。

```
<HTML><HEAD><TITLE>Cisco Systems Inc. Web Authentication Redirect</TITLE><META
http-equiv="Cache-control" content="no-cache"><META http-equiv="Pragma"
content="no-cache"><META http-equiv="Expires" content="-1"><META http-equiv="refresh"
content="1; URL=https://1.1.1.1/login.html?redirect=cisco-lwapp-controller.qqq.qqqqq.
cube.net/"></HEAD></HTML>
```

次に、クライアントは 3 ウェイ ハンドシェイクによる TCP 接続を閉じます。



クライアントは、リダイレクト URL への HTTPS 接続を開始します。クライアントはこの URL をコントローラの仮想 IP アドレスである 1.1.1.1 に送信します。 SSL トンネルを開始するため、クライアントはサーバ証明書を検証するか、または無視する必要があります。 この例では、証明書が自己署名証明書であるため、クライアントはそれを無視します。 ログイン Web ページがこの SSL トンネルを経由して送信されます。 トランザクションは、パケット 42 から始まります。



ワイヤレス LAN コントローラの仮想 IP アドレスのドメイン名を定義するオプションがあります。 仮想 IP アドレスにドメイン名を設定する場合、このドメイン名は、クライアントからの HTTP GET パケットへの応答の際の HTTP OK パケットの中でコントローラから返されます。 次に、このドメイン名の DNS 解決を行う必要があります。DNS 解決によって IP アドレスを取得したら、クライアントはその IP アドレス (コントローラの仮想インターフェイスに設定された IP) を使用して TCP セッションを開始しようとします。

最終的に、Web ページがトンネルを経由してクライアントに送られ、ユーザはユーザ名/パスワードを SSL トンネルを経由して送信します。

次の 3 つの方法のいずれかによって、Web 認証が実行されます。

- 内部 Web ページ (デフォルト) を使用した Web 認証。 デフォルト Web ページの使用の詳細については、「デフォルト Web 認証ログイン ページの選択」を参照してください。
- カスタマイズしたログイン ページを使用した Web 認証。 カスタマイズしたログイン ページの使用の詳細については、「カスタマイズした Web 認証ログイン ページの作成」を参照してください。
- 外部 Web サーバが提供するログイン ページを使用した Web 認証。 外部 Web サーバが提供するログイン ページの使用の詳細については、「外部 Web サーバが提供するカスタマイズした Web 認証ログインページの使用」を参照してください。

注: カスタマイズされた Web 認証バンドルでは、ファイル名が最大 30 文字に制限されます。 バンドル内のすべてのファイル名が 30 文字以内であることを確認する。

注: WLC リリース 7.0 以降では、WLAN で Web 認証がイネーブルにされていて、かつ CPU ACL

ルールがある場合、クライアントが認証されていない WebAuth_Reqd 状態である間は、クライアント ベースの Web 認証ルールが常に優先されます。 クライアントが RUN 状態になると、CPU ACL ルールが適用されます。

注: したがって、CPU ACL が WLC でイネーブルである場合、次の場合には、仮想インターフェイス IP の（ANY 方向の）allow ルールが必要です。

- CPU ACL に、両方向の allow ALL ルールがない場合。
- allow ALL ルールがあるが、より優先順位の高い、ポート 443 または 80 に対する DENY ルールがある場合。

注: 仮想 IP の allow ルールは、TCP プロトコルおよびポート 80（Secureweb がディセーブルの場合）またはポート 443（Secureweb がイネーブルの場合）に対してでなければなりません。 これは、CPU ACL が設定されている場合に、クライアントの仮想インターフェイス IP アドレスへのアクセスが、正常認証をポストできるようにするために必要です。

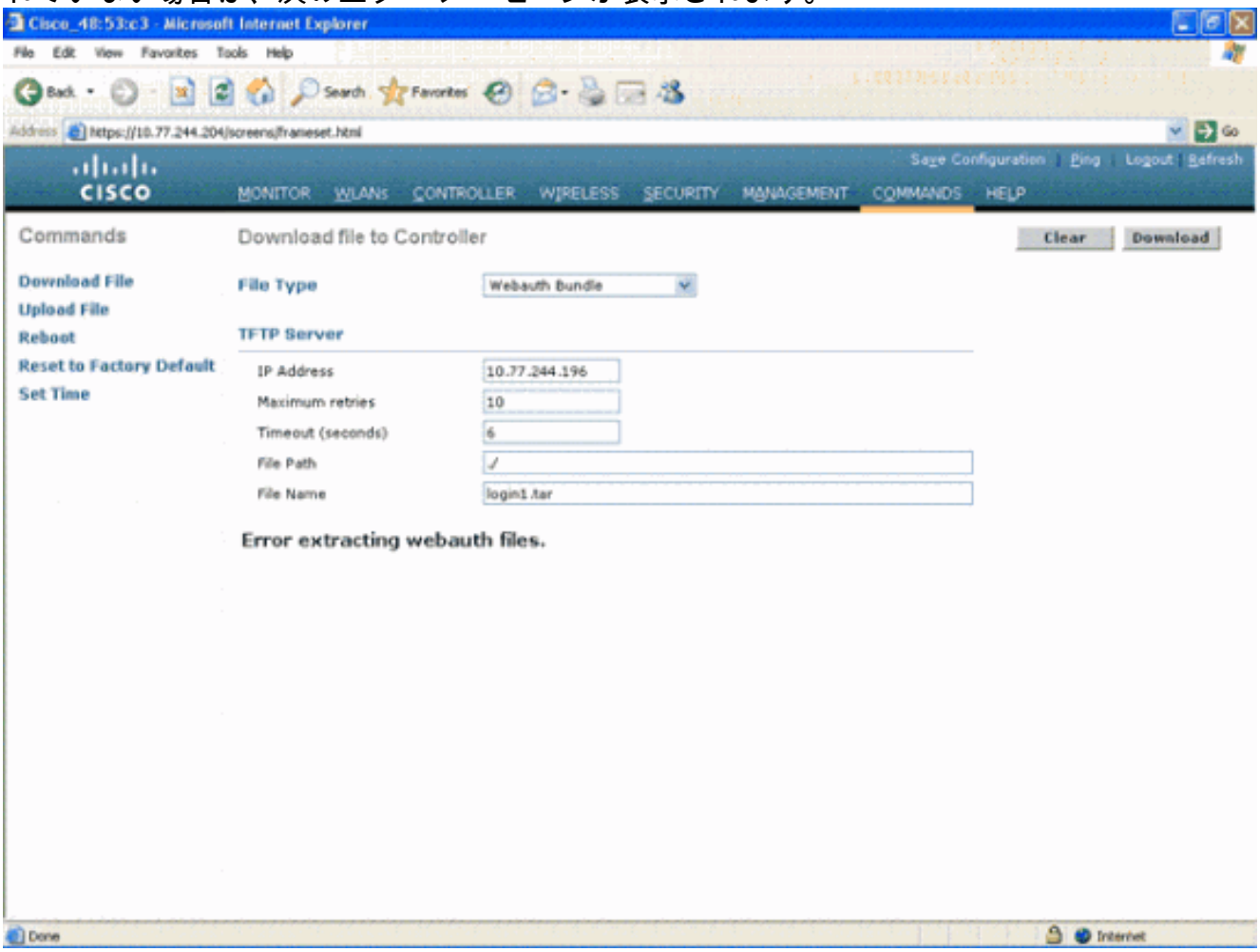
Web 認証のトラブルシューティング

Web 認証を設定した後、Web 認証機能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. クライアントが IP アドレスを取得しているかどうかを確認します。 取得していない場合は、WLAN の **DHCP Required** をオフにして、ワイヤレス クライアントに固定 IP アドレスを割り当てます。 これによって、アクセス ポイントの割り当てが見込まれます。 『*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（DHCP 関連問題のトラブルシューティングの場合）*』の「*IP アドレッシングの問題*」セクションを参照してください。
2. バージョン 3.2.150.10 よりも前の WLC で Web 認証ウィンドウに移動するには、手動で **https://1.1.1.1/login.html** を入力する必要があります。プロセスの次のステップは、Web ブラウザでの URL の DNS 解決です。 WLAN クライアントが、Web 認証用に設定された WLAN に接続したとき、クライアントは DHCP サーバから IP アドレスを取得します。 ユーザはブラウザを開始し、Web サイトのアドレスを入力します。 クライアントは、DNS 解決を実行して Web サイトの IP アドレスを取得します。 ここで、クライアントがその Web サイトにアクセスしようとすると、WLC はクライアントの HTTP Get セッションをインターセプトし、ユーザを Web 認証ログイン ページにリダイレクトします。
3. したがって、リダイレクションが機能するように、クライアントが DNS 解決を実行できることを確認します。 Windows で、[Start] > [Run] を順に選択し、**CMD** を入力してコマンド ウィンドウを開きます。「nslookup www.cisco.com」を実行し、IP アドレスが返されるかどうかを確認します。Mac または Linux の場合は、 ターミナル ウィンドウを開き、「nslookup www.cisco.com」を実行して、IP アドレスが返されるかどうかを確認します。クライアントが DNS 解決を取得していないと思われる場合は、次のいずれかを実行します。URL の IP アドレスを入力します（例：http://www.cisco.com は http://198.133.219.25 です）。https://<Virtual_interface_IP_Address>/login.html を使用して、コントローラの Web 認証ページに直接アクセスを試みます。 一般的に、このページは http://1.1.1.1/login.html です。この URL の入力によって、Web ページが起動される場合、 DNS の問題である可能性が最も高くなります。 証明書の問題である可能性もあります。 デフォルトでは、コントローラは自己署名証明書を使用しますが、多くの Web ブラウザは、自己署名証明書の使用に警告を出します。
4. カスタマイズされた Web ページを使用する Web 認証の場合、カスタマイズされた Web ペ

ージの HTML コードが適切であることを確認します。サンプル Web 認証スクリプトは、シスコのソフトウェア ダウンロードからダウンロードできます。 たとえば 4400 コントローラの場合、[Products] > [Wireless] > [Wireless LAN Controller] > [Standalone Controllers] > [Cisco 4400 Series Wireless LAN Controllers] > [Cisco 4404 Wireless LAN Controller] > [Software on Chassis] > [Wireless Lan Controller Web Authentication Bundle-1.0.1] の順に選択し、**webauth_bundle.zip** ファイルをダウンロードします。ユーザのインターネット ブラウザがカスタマイズされたログイン ページにリダイレクトされるときに、次のパラメータが URL に追加されます。ap_mac：無線ユーザが関連付けられているアクセス ポイントの MAC アドレス。switch_url：ユーザ クレデンシャルの送信先コントローラの URL。redirect：認証に成功した後、ユーザがリダイレクトされる URL。statusCode：コントローラの Web 認証サーバから返されるステータス コード。wlan：無線ユーザが関連付けられている WLAN SSID。次のステータス コードが使用できます。ステータス コード 1：「ログインしました。 特にアクションは必要ありません。」ステータス コード 2：「Web ポータルに対する認証が設定されていません。 特にアクションは必要ありません。」ステータス コード 3：「指定されたユーザ名は、今回は使用できません。 あるいは、そのユーザ名はすでにシステムにログインしている可能性があります。」ステータス コード 4：「遮断されました。」ステータス コード 5：「入力されたユーザ名とパスワードが無効です。 再試行してください。"

5. カスタマイズされた Web ページの表示に必要なすべてのファイルおよび画像は、WLC にアップロードする前に .tar ファイルにバンドルする必要があります。 tar バンドルファイルに含まれるファイルの 1 つが login.html であることを確認します。 login.html ファイルが含まれていない場合は、次のエラー メッセージが表示されます。



カスタマイズされた Web 認証ウィンドウの作成方法については、「ワイヤレス LAN コントローラ Web 認証の例」の「カスタマイズされた Web 認証のガイドライン」セクションを参

照してください。**注:** 大容量ファイルと長い名前のファイルでは、抽出エラーが起こります。 画像は .jpg フォーマットをお勧めします。

6. Web 認証の使用に推奨されるブラウザは Internet Explorer 6.0 SP1 以降です。 その他のブラウザでは、機能する場合としない場合があります。
7. WLC のカスタマイズされた Web ページは本質的に HTML スクリプトであるため、クライアント ブラウザで、**Scripting** オプションがブロックされていないことを確認します。 セキュリティ上の理由から、IE 6.0 では、デフォルトでこのオプションがディセーブルにされています。**注:** ユーザ用にポップアップ メッセージを設定している場合は、ブラウザでポップアップ ブロッカーをディセーブルにする必要があります。**注: https** サイトをブラウズする場合、リダイレクションは機能しません。 詳細は、Cisco Bug ID CSCar04580（登録ユーザ専用）を参照してください。
8. WLC の**仮想インターフェイス**に**ホスト名**を設定した場合、仮想インターフェイスのホスト名に対して DNS 解決が使用できることを確認します。**注:** 仮想インターフェイスに **DNS ホスト名**を割り当てるには、WLC GUI で [Controller] > [Interfaces] メニューの順に移動します。
9. 場合によっては、クライアント コンピュータにインストールされているファイアウォールによって Web 認証ログイン ページがブロックされることがあります。 ログイン ページへのアクセスを試みる前に、ファイアウォールをディセーブルにしてください。 Web 認証が完了した後は、ファイアウォールを再びイネーブルにしても問題ありません。
10. トポロジ/ソリューション ファイアウォールは、クライアントおよび Web 認証サーバの間に、ネットワークに応じて配置できます。 各ネットワークの設計または実装ソリューションと同様に、エンドユーザはネットワークのファイアウォールにおいて次のポートが許可されていることを確認する必要があります。
11. Web 認証が実行されるには、クライアントはまず、WLC で適切な WLAN と関連付けられる必要があります。 クライアントが WLC に関連付けられているかどうかを確認するには、WLC で [Monitor] > [Clients] メニューに順に移動します。 クライアントが有効な IP アドレスを持っているかどうか確認します。
12. Web 認証が完了するまで、クライアント ブラウザのプロキシ設定をディセーブルにします。
13. デフォルトの Web 認証方式は PAP です。 RADIUS サーバで PAP 認証が機能するように許可されていることを確認します。 クライアント認証の状態を確認するために、RADIUS サーバからのデバッグ メッセージとログ メッセージを確認します。 WLC で RADIUS からのデバッグを表示するには、**debug aaa all** コマンドを使用します。
14. コンピュータのハードウェア ドライバを製造業者の Web サイトから取得した最新コードにアップデートします。
15. サプリカント（ラップトップのプログラム）の設定を確認します。
16. Windows に組み込みの Windows Zero Config サプリカントを使用する場合：最新のパッチがインストールされていることを確認します。サプリカントでデバッグを実行します。
17. クライアントのコマンド ウィンドウで、EAPOL（WPA+WPA2）および RASTLS のログをオンにします。[Start] > [Run] > [CMD] を順に実行して、次を実行します。`netsh ras set tracing eapol enable`

    `netsh ras set tracing rastls enable`ログをディセーブルにするには同じコマンドを実行しますが、enable の部分を disable に置き換えます。 XP の場合は、すべてのログは、C:\Windows\tracing に置かれます。
18. ログイン Web ページがまだない場合は、次の出力を 1 台のクライアントから収集して分析します。

```
debug client <mac_address in format xx:xx:xx:xx:xx:xx>
debug dhcp message enable
debug aaa all enable
debug dot1x aaa enable
```

```
debug mobility handoff enable
```

19. これらの手順を実行しても問題が解決しない場合は、次のデバッグを収集し、TAC Service Request Tool（登録ユーザ専用）を使用して、サービス要求をオープンしてください。

```
debug pm ssh-appgw enable
debug pm ssh-tcp enable
debug pm rules enable
debug emweb server enable
debug pm ssh-engine enable packet <client ip>
```

関連情報

- ワイヤレス LAN コントローラの Web 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
- テクニカルサポートとドキュメント - Cisco Systems