WPA 設定の概要

内容

概要

このドキュメントでは、Wi-Fi Alliance のメンバーが使用する暫定セキュリティ標準である Wi-Fi Protected Access（WPA）の設定例について説明しています。

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。

- ワイヤレス ネットワークとワイヤレスのセキュリティ問題に関する全般的な知識
- Extensible Authentication Protocol（EAP）セキュリティ方式に関する知識

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いています。

- Cisco IOS®ソフトウェアベースのアクセスポイント(AP)
- Cisco IOS ソフトウェア リリース 12.2(15)JA 以降**注：WPAが**Cisco IOSソフトウェアリリース12.2JA以降でサポートされている場合でも、最新のCisco IOSソフトウェアリリースを使用することをお勧めします。最新の Cisco IOS ソフトウェア リリースを入手するには、ダウン

ロード（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。
- WPA 準拠の Network Interface Card（NIC; ネットワーク インターフェイス カード）と、そのカードの WPA 準拠のクライアント ソフトウェア

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景理論

WEP などのワイヤレス ネットワークのセキュリティ機能は脆弱です。Wi-Fi Alliance（または WECA）インダストリ グループは、無線ネットワーク向けの次世代の暫定セキュリティ標準を策定しました。この標準は、IEEE で 802.11i 標準が批准されるまでの間、脆弱性に対処するものです。

この新しいスキームは、現在の EAP/802.1x 認証とダイナミック鍵管理を元に構築されていて、より強力な暗号化機能が追加されます。クライアント デバイスと認証サーバ間に EAP/802.1x アソシエーションが確立された後、AP と WPA 準拠のクライアント デバイス間で WPA 鍵管理がネゴシエートされます。

Cisco AP 製品では、レガシーな WEP ベースの EAP クライアント（レガシーまたは鍵なしの管理）が WPA クライアントとともに動作するハイブリッド設定も提供しています。この設定は移行モードと呼ばれます。移行モードによって、段階的に WPA への移行を進めることができます。このドキュメントでは、移行モードについては説明していません。WPA だけでセキュリティ保護されたネットワークの概要を紹介しています。

大企業または会社レベルのセキュリティ問題に加え、WPA では、small office, home office（SOHO; スモール オフィス、ホームオフィス）や家庭用無線ネットワーク向けの Pre-Shared Key（PSK; 事前共有鍵）バージョンである WPA-PSK も提供しています。Cisco Aironet Client Utility（ACU）は WPA-PSK をサポートしていません。Microsoft Windows の Wireless Zero Configuration ユーティリティはほとんどの無線カードの WPA-PSK に対応しており、次のユーティリティも同様に対応しています。

- Meetinghouse Communications の AEGIS Client**注：Meetinghouse AEGIS製**品ラインのEOSおよびEOLの発表を参照してください。
- Funk Software の Odyssey Client**注：Juniper Networksの**カスタマーサポートセンターを参照してください 。
- 一部製造業者が提供する OEM クライアント ユーティリティ

次の場合、WPA-PSK を設定できます。

- Encryption Manager タブで、暗号 Temporal Key Integrity Protocol（TKIP）として Encryption Mode を定義した場合。
- GUI の Service Set Identifier (SSID) タブで、認証タイプ、認証鍵管理の使用、および事前共有鍵を定義した場合。
- Server Manager タブでの設定は不要です。

command-line interface（CLI; コマンドライン インターフェイス）から WPA-PSK をイネーブルにするには、次のコマンドを入力します。設定モードから開始します。

```
AP(config)#interface dot11Radio 0
```

```
AP(config-if)#encryption mode ciphers tkip
AP(config-if)#ssid ssid_name
AP(config-if-ssid)#authentication open
AP(config-if-ssid)#authentication key-management wpa
AP(config-if-ssid)#wpa-psk ascii pre-shared_key
```

注：このセクションでは、WPA-PSKに関連する設定のみを提供します。設定は、WPA-PSK をイネーブルにする方法の説明のためにだけ提供されており、このドキュメントの焦点ではありません。このドキュメントでは、WPA の設定方法について説明しています。

表記法

ドキュメント表記の詳細については、『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。

設定

WPA は、現在の EAP/802.1x 方式をベースに構築されています。このドキュメントでは、WPA を組み込むための設定を追加する前に、Light EAP（LEAP）、EAP、または Protected EAP（PEAP）がすでに設定されていることを前提としています。

この項では、この文書で説明する機能を設定するために必要な情報を提供します。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク EAP または EAP を使用したオープン認証

EAP/802.1x ベースの認証方式では、ネットワーク EAP と EAP を使用したオープン認証の違いについて疑問に思われるかもしれません。これらの項目は、管理パケットおよびアソシエーション パケットのヘッダー内にある Authentication Algorithm フィールドの値を指しています。無線クライアントのほとんどの製造業者は、このフィールドの値を 0（オープン認証）に設定しており、後のアソシエーション プロセスで EAP 認証を行いたいという要望を通知します。シスコは、アソシエーションの始めから、ネットワーク EAP フラグを使ってこの値を別の方法で設定します。

ネットワークに次のようなクライアントがある場合には、このリストで示す認証方式を使用してください。

- Cisco のクライアント：ネットワーク EAP を使用する。
- サードパーティのクライアント（Cisco Compatible Extensions（CCX）準拠の製品を含む）：EAP によるオープン認証を使用する。
- Cisco とサードパーティのクライアントの両方：ネットワーク EAP と EAP によるオープン認証の両方を選択する。

CLI での設定

このドキュメントでは、次の構成を使用します。

- 正常に動作している既存の LEAP 設定
- Cisco IOS ソフトウェアベースの AP 向けの Cisco IOS ソフトウェア リリース 12.2(15)JA

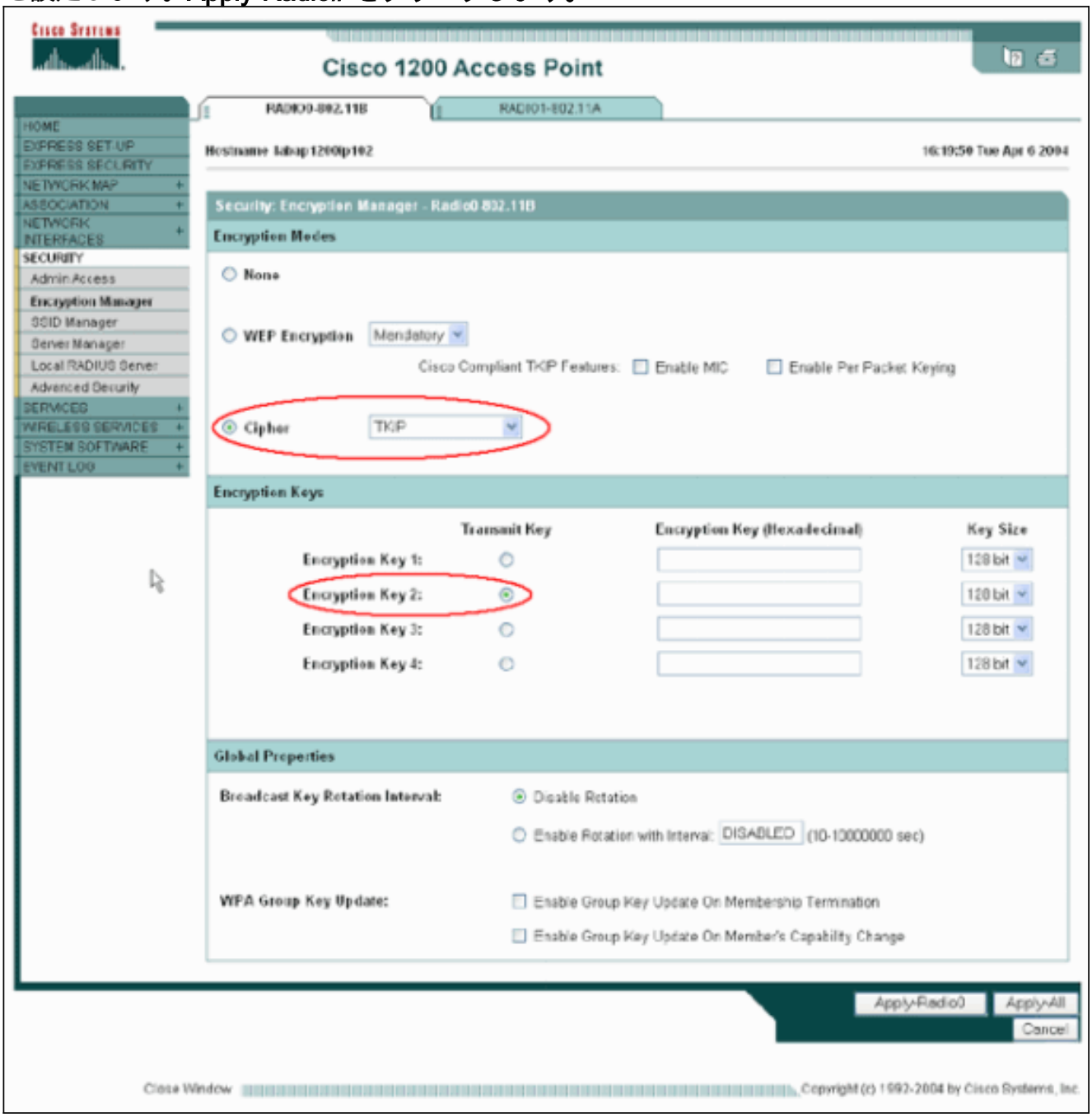
AP

```
ap1#show running-config
 Building configuration...
 .
 .
 .
aaa new-model
!
aaa group server radius rad_eap
 server 192.168.2.100 auth-port 1645 acct-port 1646
.
.
aaa authentication login eap_methods group rad_eap
.
.
.
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers tkip
!--- This defines the cipher method that WPA uses. The
TKIP !--- method is the most secure, with use of the Wi-
Fi-defined version of TKIP. ! ssid WPAlabap1200
authentication open eap eap_methods
!--- This defines the method for the underlying EAP when
third-party clients !--- are in use.     authentication
network-eap eap_methods
!--- This defines the method for the underlying EAP when
Cisco clients are in use.     authentication key-
management wpa
!--- This engages WPA key management. ! speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 rts threshold 2312
channel 2437 station-role root bridge-group 1 bridge-
group 1 subscriber-loop-control bridge-group 1 block-
unknown-source no bridge-group 1 source-learning no
bridge-group 1 unicast-flooding bridge-group 1 spanning-
disabled . . . interface FastEthernet0 no ip address no
ip route-cache duplex auto speed auto bridge-group 1 no
bridge-group 1 source-learning bridge-group 1 spanning-
disabled ! interface BVI1 ip address 192.168.2.108
255.255.255.0 !--- This is the address of this unit. no
ip route-cache ! ip default-gateway 192.168.2.1 ip http
server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server host 192.168.2.100 auth-port 1645 acct-
port 1646 key shared_secret !--- This defines where the
RADIUS server is and the key between the AP and server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end ! end
```

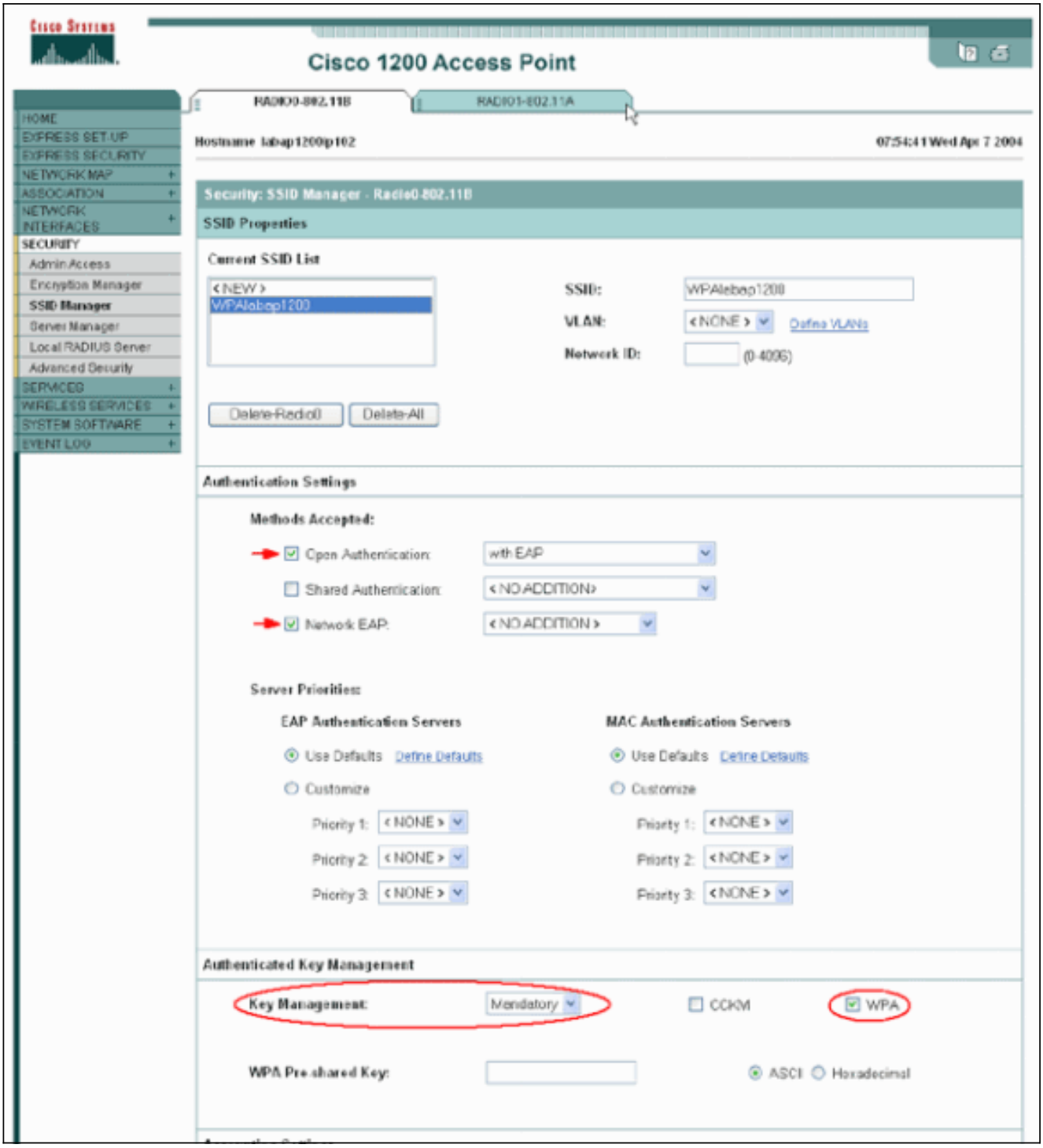
GUI での設定

WPA 用 AP を設定するには、次の手順を実行します。

1. Encryption Manager を設定するには、次の手順を実行します。TKIP の暗号化をイネーブルにします。Encryption Key 1 の値をクリアします。Transmit Key として、Encryption Key 2 を設定します。**Apply-Radio# をクリックします。**



2. SSID Manager を設定するには、次の手順を実行します。現在の SSID リストから目的の SSID を選択します。適切な認証方式を選択します。使用するクライアント カードの種類に基づいて判断します。詳細は、このドキュメントの「ネットワーク EAP または EAP を使用したオープン認証」を参照してください。WPA を追加する前に EAP が動作している場合には、おそらく変更は不要です。鍵管理をイネーブルにするには、次の手順を実行します。Key Management ドロップダウン メニューから **Mandatory** を選択します。WPA チェックボックスをオンにします。**Apply-Radio# をクリックします。**

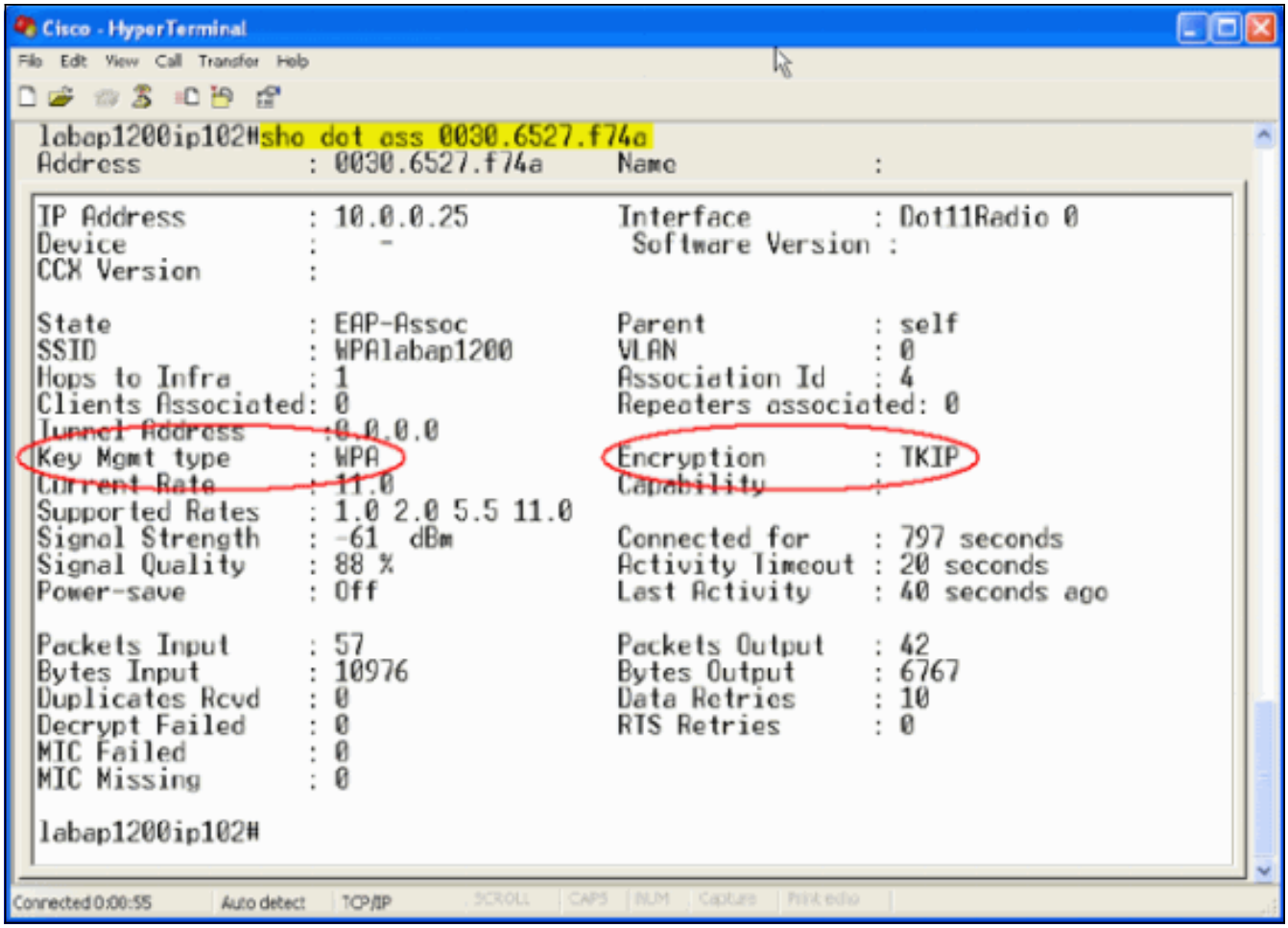


確認

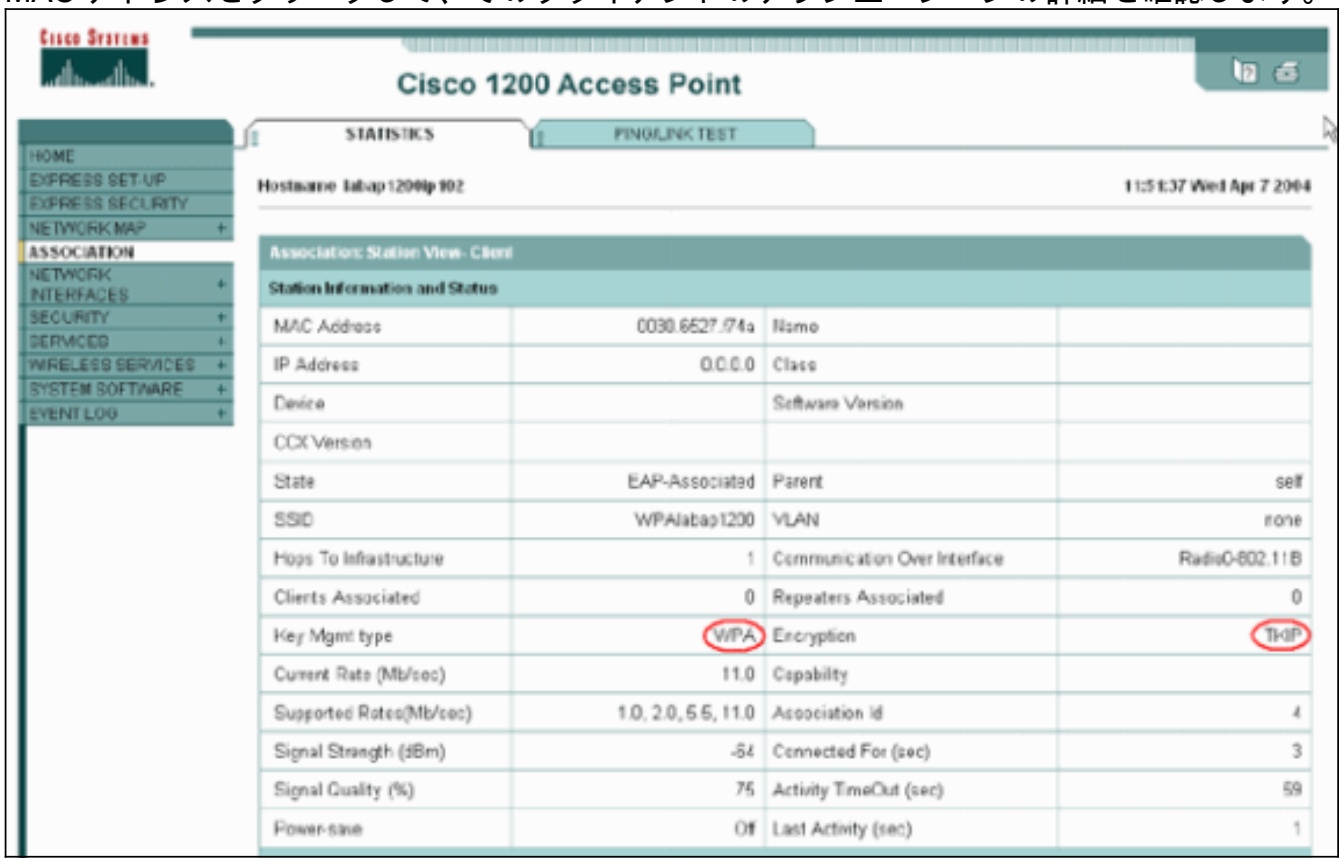
ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show dot11 association *mac_address* : 特に特定のアソシエーション クライアントに関する情報を表示します。**クライアントが、鍵管理を WPA として、暗号化を TKIP としてネゴシエートしていることを確認します。



- 特定のクライアントのアソシエーション テーブル エントリでも、鍵管理が **WPA** であり、暗号化が **TKIP** である必要があります。アソシエーション テーブルでクライアント用の特定の MAC アドレスをクリックして、そのクライアントのアソシエーションの詳細を確認します。



トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングの手順

この情報は、ここでの設定に関連するものです。設定をトラブルシューティングするには、次の手順を実行します。

1. WPA を実装する前に上記の LEAP、EAP、または PEAP 設定を十分にテストしていない場合には、次の手順を実行する必要があります。WPA 暗号化モードを一時的にディセーブルにします。適切な EAP を再度イネーブルにします。認証が機能していることを確認します。
2. クライアントの設定が AP の設定と一致していることを確認します。たとえば、AP が WPA と TKIP 用に設定されている場合、この設定がクライアントの設定と一致していることを確認します。

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。

EAP 認証が正常に終了した後、WPA 鍵管理には 4 方向のハンドシェイクが関与しています。この 4 つのメッセージを参照するには、debug コマンドを使用します。EAP が正常にクライアントを認証しない場合、またはメッセージが表示されない場合は、次の手順を実行します。

1. WPA を一時的にディセーブルにします。
2. 適切な EAP を再度イネーブルにします。
3. 認証が機能していることを確認します。

次のリストでは、debug について説明しています。

- **debug dot11 aaa manager keys**：pairwise transient key（PTK）と group transient key（GTK）がネゴシエートするときに AP と WPA クライアント間で発生するハンドシェイクを表示します。このデバッグは Cisco IOS ソフトウェア リリース 12.2(15)JA で導入されました。debug の出力がない場合には、次の項目を確認します。ターミナル モニタ **term mon** が有効であること（Telnet セッションを使用する場合）。debug がイネーブルになっていること。クライアントが WPA 用に適切に設定されていること。debug コマンドによって、PTK や GTK のハンドシェイクの確立が表示されるにもかかわらず、そのハンドシェイクを確認できない場合は、WPA サプリカント ソフトウェアが適切に設定されているかどうか、および最新バージョンであるかどうかを確認してください。
- **debug dot11 aaa authenticator state-machine**：クライアントがアソシエーションと認証を実行する際に遷移していくネゴシエーションのさまざまな状態を表示します。状態名は、それぞれの状態を示します。このデバッグは Cisco IOS ソフトウェア リリース 12.2(15)JA で導入されました。この debug コマンドは、Cisco IOS ソフトウェア リリース 12.2(15)JA 以降では、**debug dot11 aaa dot1x state-machine command** コマンドに代わるコマンドとして使用されています。
- **debug dot11 aaa dot1x state-machine**：クライアントがアソシエーションと認証を実行する際に遷移していくネゴシエーションのさまざまな状態を表示します。状態名は、それぞれの状態を示します。Cisco IOS ソフトウェア リリース 12.2(15)JA よりも前の Cisco IOS ソフトウェア リリースでは、WPA 鍵管理ネゴシエーションも表示されます。
- **debug dot11 aaa authenticator process**：ネゴシエーション関連の通信に関する問題を診断す

る場合、この debug コマンドは非常に有効です。このコマンドによって表示された詳細情報には、ネゴシエーションのそれぞれの側が送信した内容と、もう一方が応答した内容が表示されます。この debug コマンドは、**debug radius authentication コマンドと併用することもできます。**このデバッグは Cisco IOS ソフトウェア リリース 12.2(15)JA で導入されました。この debug コマンドは、Cisco IOS ソフトウェア リリース 12.2(15)JA 以降では、**debug dot11 aaa dot1x process** コマンドに代わるコマンドとして使用されています。

- **debug dot11 aaa dot1x process**：ネゴシエーション関連の通信に関する問題を診断する場合、この debug コマンドは有効です。このコマンドによって表示された詳細情報には、ネゴシエーションのそれぞれの側が送信した内容と、もう一方が応答した内容が表示されます。この debug コマンドは、**debug radius authentication コマンドと併用することもできます。** Cisco IOS ソフトウェア リリース 12.2(15)JA よりも前の Cisco IOS ソフトウェア リリースでは、WPA 鍵管理ネゴシエーションも表示されます。

関連情報

- 暗号スイートと WEP の設定
- 認証タイプの設定
- WPA2 - Wi-Fi Protected Access 2
- Wi-Fi Protected Access 2 (WPA 2) の設定例
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。