Autonomous アクセス ポイント上の WEP の設定例

内容

はじめに

このドキュメントでは、Cisco Autonomous アクセス ポイント（AP）での Wired Equivalent Privacy（WEP）の使用法と設定方法を説明します。

前提条件

要件

このドキュメントでは、WLAN デバイスへ管理接続できること、また暗号化のない環境でデバイスが正常に機能することが前提となっています。標準的な 40 ビットの WEP を設定するには、2 つ以上の相互に通信する無線装置が必要です。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS® リリース 15.2JB を実行する 1140 AP に基づいています。

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、クリアな（デフォルト）設定で作業を開始しています。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。

背景説明

WEP は 802.11 標準（Wi-Fi）に組み込まれている暗号化アルゴリズムです。WEP は機密保持

のために ストリーム 暗号 RC4 を使用し、整合性 を 保 つために 巡回冗長検査 32 (CRC-32) チェックサム を 使用 します。

標準の 64 ビット WEP は 40 ビット キー (WEP-40) を 使用 します。これは、24 ビット 初期化 ベクトル (IV) と 連結 して RC4 キー を 形成 します。 64 ビット WEP キーは通常、10 個の 16 進数 (base 16) 文字 (0 ~ 9、 A ~ F) からなる 文字列 として 入力 されます。 各文字は4ビットを表し、4ビットを10桁ずつ40ビットになります。24ビットのIVを追加すると、完全な64ビットのWEPキーが生成されます。

128 ビット WEP キーは通常、26 個の 16 進数文字からなる文字列として入力されます。4ビットの26桁はそれぞれ104ビットになります。24ビットのIVを追加すると、完全な128ビットのWEPキーが生成されます。ほとんどのデバイスでは、ユーザがこのキーを 13 個の ASCII 文字として入力できます。

認証方式

WEPでは、オープンシステム認証と共有キー認証の2つの認証方法を使用できます。

オープン システム認証では、WLAN クライアントは認証のためにクレデンシャルを AP に提供する必要がありません。クライアントは AP を認証し、関連付けを試行できます。実際には認証は行われません。続いて WEP キーを使用してデータ フレームを暗号化できます。この時点で、クライアントには正しいキーが必要です。

共有キー認証では、4 段階のチャレンジ/レスポンス ハンドシェイクでの認証に WEP キーが使用されます。

1. クライアントは AP に認証要求を送ります。
2. AP がクリア テキスト の チャレンジ で 応答 します。
3. クライアントが、設定されている WEP キーを使用してチャレンジ テキストを暗号化し、別の認証要求で応答します。
4. AP が応答を復号化します。応答がチャレンジ テキストに一致する場合、AP が肯定応答を送信します。

認証および関連付けの後で、RC4 でデータ フレームを暗号化するために事前共有 WEP キーも使用されます。

一見すると、オープン システム認証では実際の認証が行われないために、共有キー認証のほうがセキュアであるように見えます。ただし、実際はその逆です。共有キー認証でチャレンジ フレームをキャプチャすると、ハンドシェイクに使用されるキーストリームを得ることができます。このため、WEP 認証には共有キー認証ではなく、オープン システム認証を使用することを推奨します。

WEP の問題を解決するため、Temporal Key Integrity Protocol (TKIP) が作成されました。WEP と同様に、TKIP は RC4 暗号化を使用します。ただし TKIP では、既知の WEP の脆弱性に対処するために、パケット単位キー ハッシュ、メッセージ整合性チェック (MIC)、ブロードキャスト キー ローテーションなどの手法が追加され、WEP が拡張されています。TKIP は、暗号化に 128 ビット キーによる RC4 ストリーム暗号を使用し、認証に 64 ビット キーを使用します。

設定

ここでは、WEP の GUI 設定と CLI 設定について説明します。

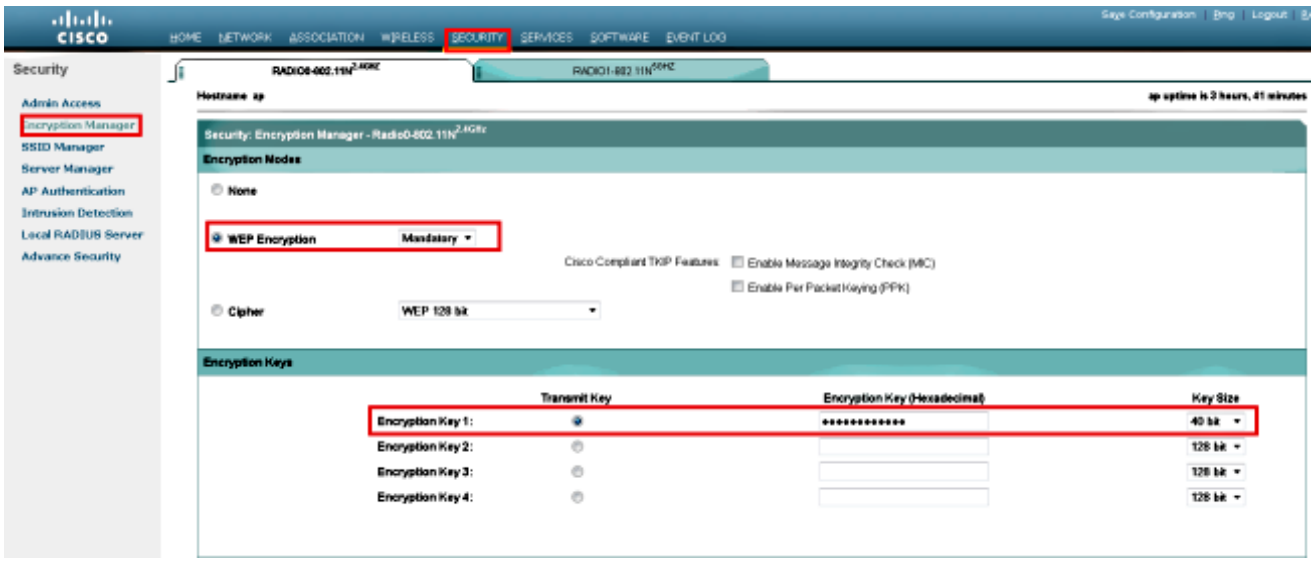
GUI での設定

GUI で WEP を設定するには、次の手順を実行します。

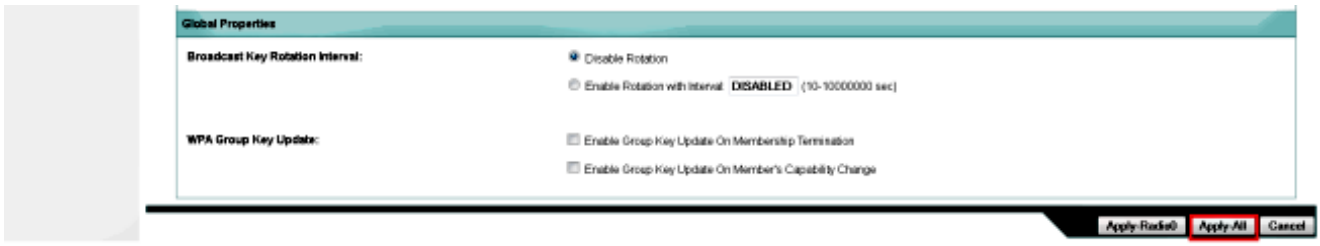
1. GUI を使用して AP に接続します。
2. ウィンドウの左側にある [Security] メニューから、スタティック WEP キーを設定する無線インターフェイスの [Encryption Manager] を選択します。
3. [Encryption Modes] の下の [WEP Encryption] をクリックし、クライアントのドロップダウン メニューから [Mandatory] を選択します。

   ステーションが使用する暗号化モードは次のとおりです。
   - [Default (No Encryption)] : クライアントがデータ暗号化なしで AP と通信する必要があります。この設定は推奨されません。
   - [Optional] : クライアントに対しデータ暗号化ありまたはなしで AP と通信することを許可します。通常、このオプションは、シスコ以外のクライアントなど WEP 接続を行えないクライアント デバイスが 128 ビットの WEP 環境に含まれている場合に使用します。
   - [Mandatory (Full Encryption)] : クライアントが AP との通信でデータ暗号化を使用する必要があります。データ暗号化を使用しないクライアントは通信できません。この暗号化オプションは、WLAN のセキュリティを最大にする場合に推奨されます。
4. [Encryption Keys] の下で [Transmit Key] オプション ボタンをオンにし、10 桁の 16 進数キーを入力します。[Key Size] が [40 bit] に設定されていることを確認します。

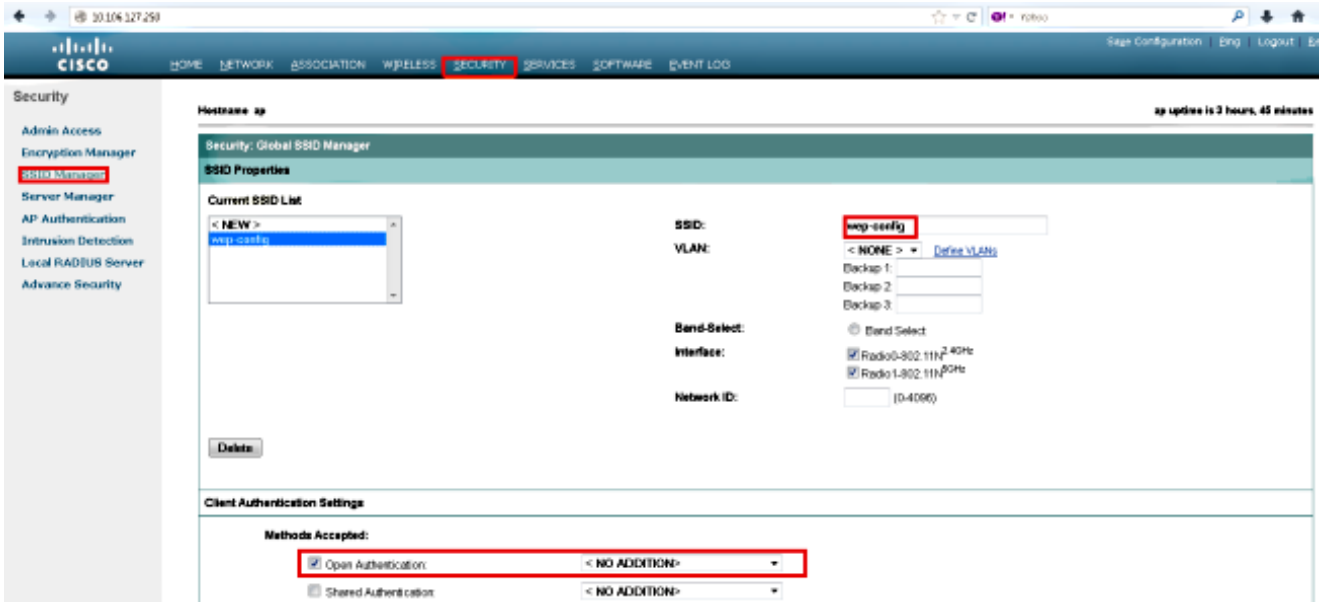
   40 ビット WEP キーには 10 桁の 16 進数値、また 128 ビットの WEP キーには 26 桁の 16 進数値を入力します。キーには次の文字を任意に組み合わせることができます。
   - 0 ~ 9
   - a 〜 f
   - A ~ F



5. [Apply-All] をクリックして、両方の無線に設定を適用します。



6. [Open Authentication] を使用してサービス セット識別子（SSID）を作成し、[Apply] をクリックして、両方の無線でその ID を有効にします。



7. ネットワークに移動し、[2.4 GHz] と [5 GHz] の両方の無線をオンにして、これらを実行します。

CLI での設定

CLI で WEP を設定するには、この項の情報を参照してください。

```
<#root>

ap#

show run


Building configuration...

Current configuration : 1794 bytes
!
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$kxBl$OhRR4QtTUVDUA9GakGDFs1
!
no aaa new-model
ip cef
!
!
!
dot11 syslog
!
  dot11 ssid wep-config
  authentication open
  guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 0802455D0A16
!
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
```

```
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1

 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
 no keepalive
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address dhcp
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.106.127.4
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
login local
transport input all
!
end
```

確認

設定が正しく機能していることを確認するには、次のコマンドを入力します。

```
<#root>

ap#

show dot11 associations


802.11 Client Stations on Dot11Radio0:
SSID [wep-config] :
MAC Address    IP address      Device        Name           Parent         State
1cb0.94a2.f64c 10.106.127.251  unknown       -              self           Assoc
```

トラブルシュート

この項では、設定のトラブルシューティングについて説明します。

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 コマンドは、設定のトラブルシューティングに役立ちます。

- debug dot11 events：すべての dot1x イベントのデバッグを有効にします。
- debug dot11 packets：すべての dot1x パケットのデバッグを有効にします。

クライアントが WLAN に適切に関連付けられた時点を示すログの例を次に示します。

```
*Mar  1 02:24:46.246: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
1cb0.94a2.f64c Associated KEY_MGMT[NONE]
```

クライアントが正しくないキーを入力すると、次のエラーが表示されます。

```
*Mar  1 02:26:00.741: %DOT11-4-ENCRYPT_MISMATCH: Possible encryption key
mismatch between interface Dot11Radio0 and station 1cb0.94a2.f64c
*Mar  1 02:26:21.312: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating
Station 1cb0.94a2.f64c Reason: Sending station has left the BSS
*Mar  1 02:26:21.312: *** Deleting client 1cb0.94a2.f64c
```

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。