Autonomous アクセス ポイント上の WEP の設 定例

内容

<u>はじめに</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>認証方式</u>
<u>設定</u>
<u>GUI での設定</u>
<u>CLI での設定</u>
<u>確認</u>
<u>トラブルシュート</u>

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 15.2}JB 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<u>機密保持</u>

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

標準の 64 ビット WEP は <u>40 ビット キー(WEP-40)</u>を<u>使用</u>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 <u>16 進数(base 16)</u>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<u>クリア テキスト の チャレンジ で 応答 します。</u>
- 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。

ー見すると、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

	RADIO8-002.11N2	HORE I	RADIO1-802.11N ^{50HZ}		
-	ostname ap				ap uptime is 3 hours, 4
iger	Security: Encryption Manage	r - Radio0-802.11N ^{2.4GHz}			
	Encryption Nodes				
an	C None				
tion					
v	* WEP Encryption	Mandalary *	Cisco Compliant TXIP Easterney	Evable Manages Integer: Charle B&Co	
			Calco Comprises Trop Personal	Enable Rectargle Revents (Second PER)	
	Cipher	WEP 128 bit	•		
	Encryption Keys				
			Transmit Key	Encryption Key (Hexadecima)	Key Size
		Encryption Key 1:	•	*******	40 bk 💌
		Encryption Key 2:	0		128 bit -
		Encryption Key 3:	0		128 bit =
		Encryption Key 4:	0		128 bit -

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

Global Properties	
Broadcast Key Rotation Interval:	Disable Rotation
	Enable Rotation with Internal DISABLED (10-10000000 sec)
	_
WPA Group Key Update:	Enable Group Key Update On Membership Termination
	Enable Group Key Update On Member's Capability Change
	Ander Frei Kall

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。

 In the second sec			슈 ㅋ C Of • roteo	P 🖡 👬
cisco	HOME NETWORK ASSOCIATION WIRELESS SECURITY	259.vices 20PTWARE EVENTLOG		Sage Configuration Bing Logout B
Security	Hostname ap			ay uptime is 3 hours, 45 minutes
Admin Access	Security: Global SSID Manager			
SSID Manager	SSID Properties			
Server Manager	Current SSID List			
AP Authentication	< NEW> *	SSD:	wep-coolig	
Intrusion Detection	wep-cashg	VLAN	< NONE > Define VLANs	
Advance Security			Backup 1: Backup 2	
	*		Beckap 3	
		Band-Select:	Band Select	
		interface:	Radio0-302.11N ^{2.40Hz} Radio1-302.11N ^{8CHz}	
		Network ID:	(0-4096)	
	Dakta			
	Client Authentication Settings			
	Nethods Accepted:			
	Open Authentication:	< NO ADDITION> -		
	Shared Authentication:	< NO ADDITION> *	-	

Guest Modelinfrastructure SSID Settings	
Radio0-402.11N ^{2.4GHz} :	
Set Beacon Mode:	Single BSSD Set Single Geest Mode SSD wep-config •
	© Mage BSSD
Set Infrastructure SSID:	< NONE > • E Force infrastructure Devices to associate only to this SSID
Radio1-802.11N ^{5GRz} :	
Set Beacce Mode:	Single BSSID Set Single Guest Mode SSID. wep-could *
	C Multiple BSSD
Set Infrastructure SSID:	< NONE > • E Force infrastructure Devices to associate only to this SSID
	Apply G

- 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
1
hostname ap
!
1
logging rate-limit console 9
enable secret 5 $1$kxBl$OhRR4QtTUVDUA9GakGDFs1
1
no aaa new-model
ip cef
!
!
1
dot11 syslog
!
  dot11 ssid wep-config
  authentication open
  guest-mode
1
!
crypto pki token default removal timeout 0
1
!
username Cisco password 7 0802455D0A16
I
I
bridge irb
I
1
1
interface Dot11Radio0
no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 I
 ssid wep-config
 1
 antenna gain O
 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
I
interface Dot11Radio1
no ip address
 1
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 1
 ssid wep-config
 1
 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
L
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
I
interface BVI1
 ip address dhcp
ļ
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
Т
Т
1
line con 0
line vty 0 4
login local
transport input all
1
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 State1cb0.94a2.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。