WEP auf einem autonomen Access Point - Konfigurationsbeispiel

Inhalt

Einleitung

In diesem Dokument wird die Verwendung und Konfiguration von Wired Equivalent Privacy (WEP) auf einem unabhängigen Cisco Access Point (AP) beschrieben.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie eine administrative Verbindung zu den WLAN-Geräten herstellen können und dass die Geräte in einer unverschlüsselten Umgebung normal funktionieren. Um ein standardmäßiges 40-Bit-WEP zu konfigurieren, müssen zwei oder mehr Funkeinheiten miteinander kommunizieren.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem Access Point der Serie 1140, auf dem Cisco IOS® Release 15.2JB ausgeführt wird.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

WEP ist der in den 802.11-Standard (Wi-Fi) integrierte Verschlüsselungsalgorithmus. WEP verwendet die Stream-Verschlüsselung RC4 zur Vertraulichkeit und die Cyclic Redundancy Check-32 (CRC-32)-Prüfsumme zur Integrität .

Das standardmäßige 64-Bit-WEP verwendet einen 40-Bit- Schlüssel (auch WEP-40 genannt), der zur

Bildung des RC4-Schlüssels mit einem 24-Bit-Initialisierungsvektor (IV) verknüpft wird. Ein 64-Bit-WEP-Schlüssel wird in der Regel als Zeichenfolge mit 10 Hexadezimalzeichen (Basis 16) (0 bis 9 und A-F) eingegeben. Jedes Zeichen steht für vier Bit, und zehn Ziffern von vier Bit entsprechen jeweils 40 Bit. Wenn Sie den 24-Bit-IV hinzufügen, wird der vollständige 64-Bit-WEP-Schlüssel erzeugt.

Ein 128-Bit-WEP-Schlüssel wird normalerweise als Zeichenfolge mit 26 Hexadezimalzeichen eingegeben. 26 Ziffern mit vier Bit entsprechen 104 Bit. Wenn Sie den 24-Bit-IV hinzufügen, wird der vollständige 128-Bit-WEP-Schlüssel erzeugt. Die meisten Geräte erlauben dem Benutzer, den Schlüssel als 13 ASCII-Zeichen einzugeben.

Authentifizierungsmethoden

Mit WEP können zwei Authentifizierungsmethoden verwendet werden: Open System Authentication und Shared Key Authentication.

Bei der offenen Systemauthentifizierung muss der WLAN-Client dem WAP keine Anmeldeinformationen für die Authentifizierung bereitstellen. Jeder Client kann sich beim Access Point authentifizieren und dann versuchen, eine Verbindung herzustellen. Im Prinzip findet keine Authentifizierung statt. Anschließend können WEP-Schlüssel verwendet werden, um Datenrahmen zu verschlüsseln. An dieser Stelle muss der Client über die richtigen Schlüssel verfügen.

Bei der Shared Key-Authentifizierung wird der WEP-Schlüssel für die Authentifizierung in einem vierstufigen Challenge-Response-Handshake verwendet:

1. Der Client sendet eine Authentifizierungsanforderung an den WAP.
2. Der Access Point antwortet mit einer Klartext- Herausforderung.
3. Der Client verschlüsselt den Abfragetext mit dem konfigurierten WEP-Schlüssel und antwortet mit einer weiteren Authentifizierungsanforderung.
4. Der WAP entschlüsselt die Antwort. Stimmt die Antwort mit dem Text der Herausforderung überein, sendet der Access Point eine positive Antwort.

Nach der Authentifizierung und Zuordnung wird auch der vorinstallierte WEP-Schlüssel verwendet, um die Datenframes mit RC4 zu verschlüsseln.

Auf den ersten Blick mag es so aussehen, als ob Shared Key Authentication sicherer ist als Open System Authentication, da letztere keine echte Authentifizierung bietet. Das Gegenteil ist jedoch der Fall. Es ist möglich, den für den Handshake verwendeten Schlüsselstrom abzuleiten, wenn Sie die Challenge-Frames in Shared Key Authentication erfassen. Daher ist es ratsam, für die WEP-Authentifizierung statt der Shared Key-Authentifizierung die Open System Authentication zu verwenden.

Das TKIP (Temporal Key Integrity Protocol) wurde erstellt, um diese WEP-Probleme zu beheben. Ähnlich wie WEP verwendet TKIP die RC4-Verschlüsselung. TKIP erweitert WEP jedoch um zusätzliche Maßnahmen wie paketbasiertes Key Hashing, Message Integrity Check (MIC) und Broadcast Key Rotation, um bekannte WEP-Schwachstellen zu beheben. TKIP verwendet die RC4-Stream-Verschlüsselung mit 128-Bit-Schlüsseln für die Verschlüsselung und 64-Bit-Schlüsseln für die Authentifizierung.

Konfigurieren

In diesem Abschnitt werden die GUI- und CLI-Konfigurationen für WEP beschrieben.

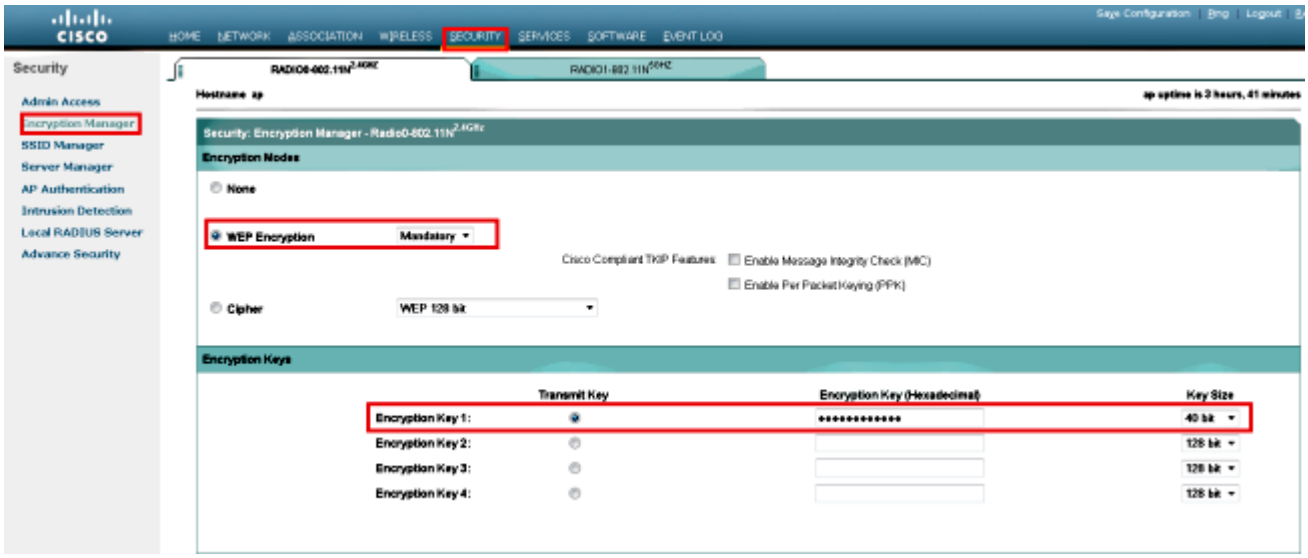
GUI-Konfiguration

Führen Sie diese Schritte aus, um WEP mit der GUI zu konfigurieren.

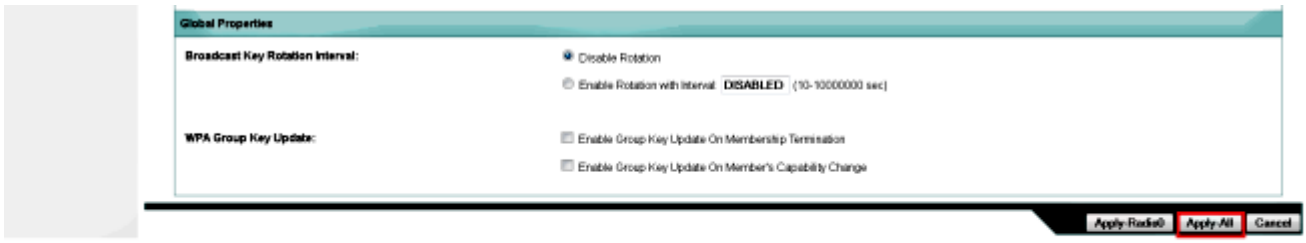
1. Stellen Sie über die Benutzeroberfläche eine Verbindung zum AP her.
2. Wählen Sie im Menü Security (Sicherheit) auf der linken Seite des Fensters für die Funkschnittstelle, für die Sie die statischen WEP-Schlüssel konfigurieren möchten, den **Verschlüsselungs-Manager aus**.
3. Klicken Sie unter Verschlüsselungsmodi auf **WEP-Verschlüsselung**, und wählen Sie **Obligatorisch** aus dem Dropdown-Menü für den Client aus.

   Die von Station verwendeten Verschlüsselungsmodi sind:
   - **Standard (keine Verschlüsselung)** - Erfordert, dass Clients ohne Datenverschlüsselung mit dem Access Point kommunizieren. Diese Einstellung wird nicht empfohlen.
   - **Optional** - Ermöglicht Clients die Kommunikation mit dem Access Point entweder mit oder ohne Datenverschlüsselung. In der Regel verwenden Sie diese Option, wenn Clientgeräte vorhanden sind, die keine WEP-Verbindung herstellen können, z. B. Clients von anderen Anbietern in einer 128-Bit-WEP-Umgebung.
   - **Obligatorisch (vollständige Verschlüsselung)** - Erfordert, dass Clients Datenverschlüsselung verwenden, wenn sie mit dem WAP kommunizieren. Clients, die keine Datenverschlüsselung verwenden, dürfen nicht kommunizieren. Diese Option wird empfohlen, wenn Sie die Sicherheit Ihres WLAN maximieren möchten.
4. Wählen Sie unter Encryption Keys (Verschlüsselungsschlüssel) das Optionsfeld **Transmit Key (Übertragungsschlüssel)** aus, und geben Sie den zehnstelligen Hexadezimalschlüssel ein. Stellen Sie sicher, dass die Schlüsselgröße auf **40 Bit** festgelegt ist.

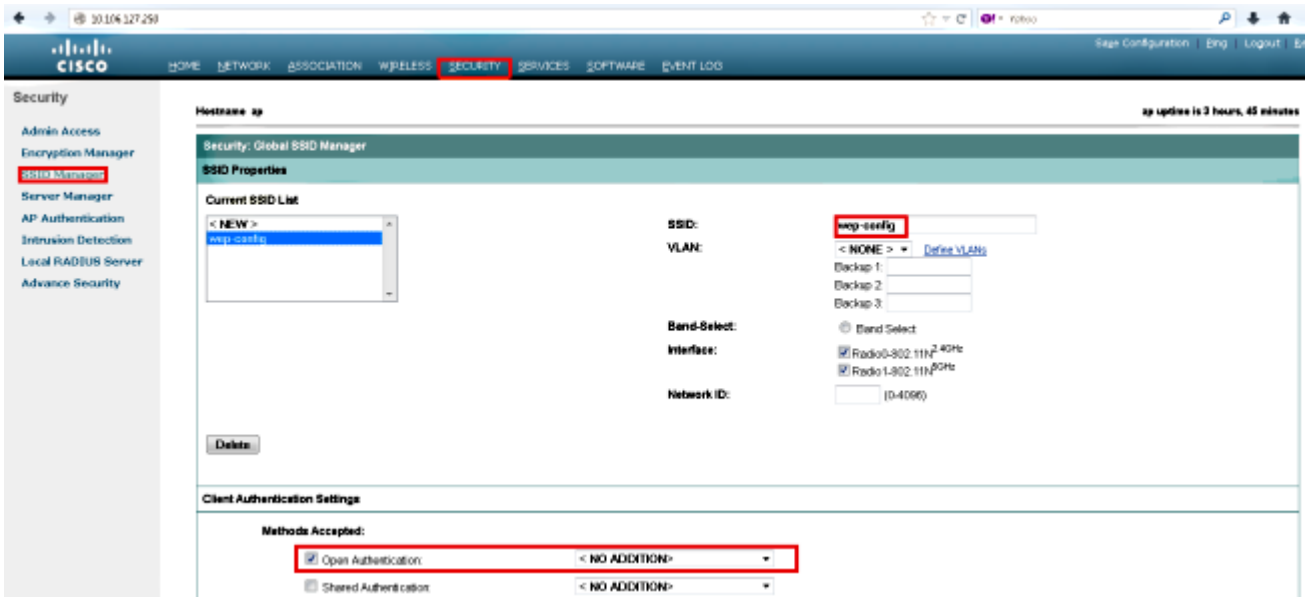
   Geben Sie 10 Hexadezimalziffern für 40-Bit-WEP-Schlüssel oder 26 Hexadezimalziffern für 128-Bit-WEP-Schlüssel ein. Bei den Tasten kann es sich um eine beliebige Kombination der folgenden Ziffern handeln:
   - 0 bis 9
   - a bis f
   - A bis F



5. Klicken Sie auf **Apply-All** (Übernehmen), um die Konfiguration für beide Funkmodule anzuwenden.



6. Erstellen Sie einen Service Set Identifier (SSID) mit **Open Authentication**, und klicken Sie auf **Apply**, um ihn für beide Funkmodule zu aktivieren.



7. Navigieren Sie zum Netzwerk, und aktivieren Sie die Funkmodule für **2,4 GHz** und **5 GHz**, um sie in Betrieb zu nehmen.

CLI-Konfiguration

In diesem Abschnitt können Sie WEP mit der CLI konfigurieren.

<#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
```

Überprüfung

Geben Sie den folgenden Befehl ein, um sicherzustellen, dass Ihre Konfiguration ordnungsgemäß funktioniert:

<#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
```

Fehlerbehebung

Verwenden Sie diesen Abschnitt, um Probleme mit Ihrer Konfiguration zu beheben.

> **Hinweis**: Lesen Sie Wichtige Informationen zu Debug-Befehlen, bevor Sie **Debug**-Befehle verwenden.

Die folgenden **Debug**-Befehle sind nützlich, um Fehler in der Konfiguration zu beheben:

- **debug dot11 events**: Aktiviert das Debugging für alle dot1x-Ereignisse.
- **debug dot11-Pakete**: Aktiviert das Debugging für alle dot1x-Pakete.

Das folgende Beispiel wird angezeigt, wenn der Client erfolgreich eine Verbindung mit dem WLAN herstellt:

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

Wenn der Client den falschen Schlüssel eingibt, wird folgender Fehler angezeigt:

```
*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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.