自治接入点上的WEP配置示例

目录

简介

本文档介绍如何在思科自主接入点(AP)上使用和配置有线等效保密(WEP)。

先决条件

要求

本文档假定您可以与WLAN设备建立管理连接，并且设备在未加密环境中正常运行。要配置标准40位WEP，您必须有两个或多个无线电单元相互通信。

使用的组件

本文档中的信息基于运行Cisco IOS®版本15.^{2}JB的1140 AP。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

WEP是内置于802.11(Wi-Fi)标准的加密算法。WEP使用数据流密码　RC4　来保证机密性，使用循环冗余校验–32　(CRC-32)校验和来保证完整性。

标准64位WEP使用40位　密钥（也称为WEP-40），该密钥与24位初始化向量　(IV)连接，以形成RC4密钥。64位WEP密钥通常作为包含10个十六进制（以16为基数）字符（0到9和A-F）的字符串输入。每个字符代表四位，四位的10位分别等于40位；如果添加24位IV，它会生成完整的64位WEP密钥。

128位WEP密钥通常作为包含26个十六进制字符的字符串输入。26位（每位4位）等于104位；如果添加24位IV，则会生成完整的128位WEP密钥。大多数设备允许用户以13个ASCII字符输入密钥。

身份验证方法

两种身份验证方法可用于WEP：开放系统身份验证和共享密钥身份验证。

使用开放系统身份验证时，WLAN客户端无需向AP提供凭证以进行身份验证。任何客户端都可以通过AP进行身份验证，然后尝试关联。实际上，不会进行身份验证。随后，可以使用WEP密钥加密数据帧。此时，客户端必须拥有正确的密钥。

使用共享密钥身份验证时，WEP密钥用于四步质询 — 响应握手：

1. 客户端向 AP 发送身份验证请求。
2. AP以明文质询回　答。
3. 客户端使用配置的WEP密钥加密质询文本，并以另一个身份验证请求进行响应。
4. AP解密响应。如果响应与质询文本匹配，则AP会发送肯定应答。

在身份验证和关联之后，也使用预共享WEP密钥来加密带有RC4的数据帧。

乍看之下，共享密钥身份验证似乎比开放系统身份验证更安全，因为后者不提供真正的身份验证。然而，事实正好相反。如果在共享密钥身份验证中捕获质询帧，则可以派生用于握手的密钥流。因此，建议使用开放式系统身份验证进行WEP身份验证，而不是使用共享密钥身份验证。

临时密钥完整性协议(TKIP)的创建是为了解决这些WEP问题。与WEP类似，TKIP使用RC4加密。但是，TKIP通过添加每数据包密钥散列、消息完整性检查(MIC)和广播密钥轮换等措施来增强WEP，以便解决已知的WEP漏洞。TKIP使用带128位密钥的RC4流密码进行加密，使用64位密钥进行身份验证。

配置

本节提供WEP的GUI和CLI配置。

GUI 配置

要使用GUI配置WEP，请完成以下步骤。

1. 通过GUI连接到AP。
2. 从窗口左侧的Security菜单中，为要配置静态WEP密钥的无线电接口选择Encryption Manager。
3. 在Encryption Modes下，单击WEP Encryption，然后从客户端的下拉菜单中选择Mandatory。

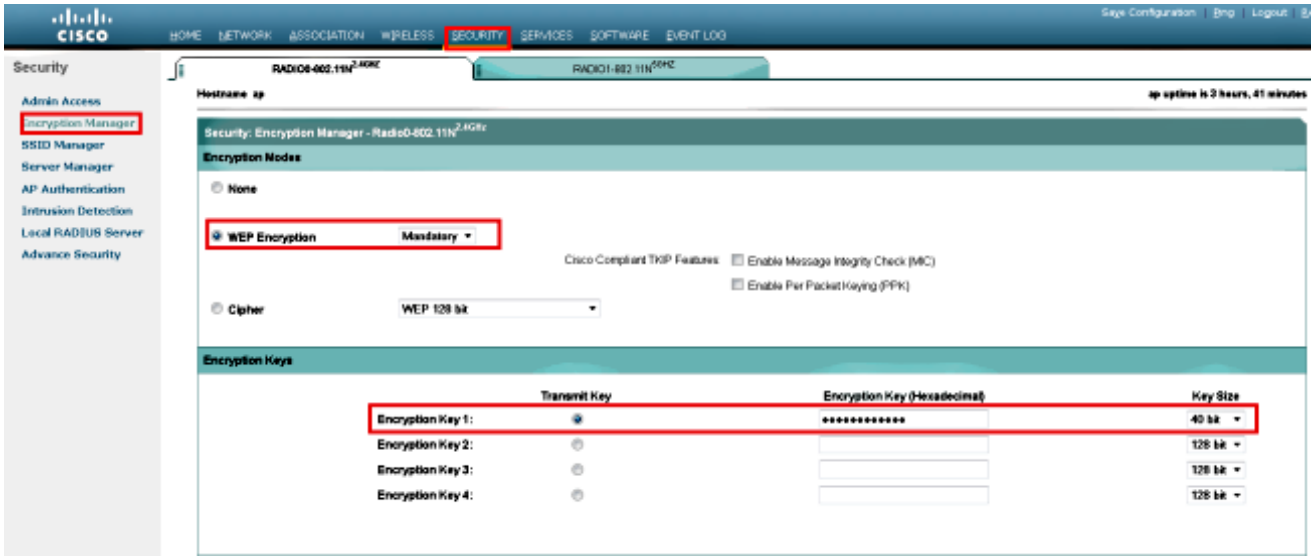
   工作站使用的加密模式包括：
   - 默认（无加密） — 要求客户端在不加密任何数据的情况下与AP通信。不建议使用此设置。
   - 可选 — 允许客户端通过数据加密或不通过数据加密与AP通信。通常，当您有无法建立WEP连接的客户端设备（例如128位WEP环境中的非思科客户端）时，使用此选项。
   - 必需(完全加密) — 要求客户端在与AP通信时使用数据加密。不使用数据加密的客户端不

允许通信。如果您希望最大限度地提高WLAN的安全性，建议使用此选项。

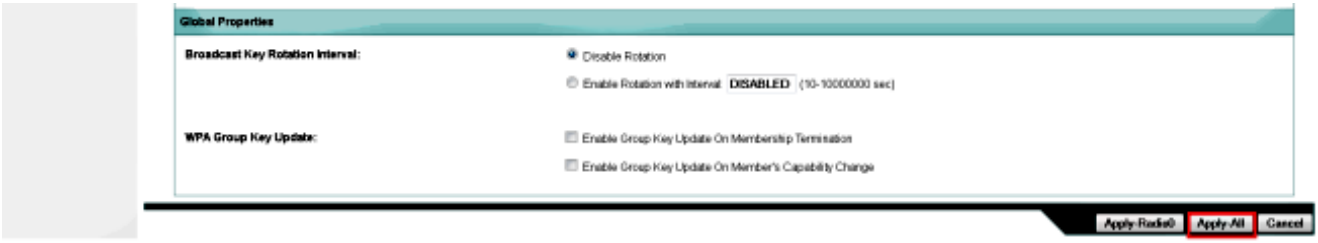
4. 在Encryption Keys下，选择Transmit Key单选按钮，然后输入10位十六进制密钥。确保密钥大小设置为40位。

   对于40位WEP密钥，输入10个十六进制数字；对于128位WEP密钥，输入26个十六进制数字。密钥可以是这些数字的任意组合：

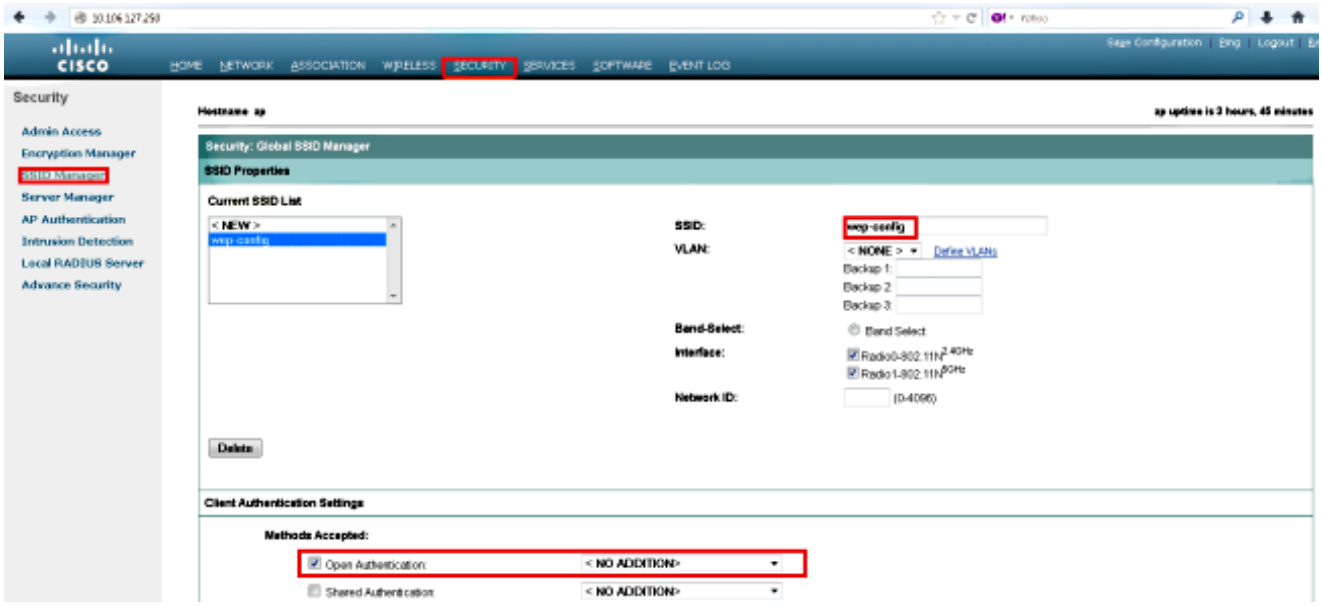
   - 0 到 9
   - a到f
   - A到F



5. 单击Apply-All以在两个无线电上应用配置。



6. 使用Open Authentication创建服务集标识符(SSID)，然后单击Apply以在两个无线电上启用它。



7. 导航到网络，并启用2.4 GHz和5 GHz的无线电以使其运行。

CLI 配置

使用此部分可以通过CLI配置WEP。

```
<#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
```

验证

输入以下命令以确认您的配置是否正常工作：

<#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
```

故障排除

使用本部分可排除配置的故障。

注意：使用debug命令之前，请参阅有关Debug命令的重要信息。

以下debug命令可用于对配置进行故障排除：

- debug dot11 events — 启用所有dot1x事件的调试。
- debug dot11 packets — 启用所有dot1x数据包的调试。

以下是客户端成功与WLAN关联时显示的日志示例：

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

当客户端输入错误的密钥时，将显示以下错误：

```
*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
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。