

在自治接入点配置示例的WEP

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[认证方法](#)

[配置](#)

[GUI 配置](#)

[CLI 配置](#)

[验证](#)

[故障排除](#)

简介

本文描述如何使用和配置在思科自治接入点(AP)的有线等效保密(WEP)。

先决条件

要求

本文假设，您能做运行联系到WLAN设备，并且设备在一个未加密环境通常作用。为了配置标准40位WEP，您必须有与彼此联络的两个或多个无线电单元。

使用的组件

运行Cisco IOS Release15.2JB的本文档中的信息根据1140个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是加密算法被建立到802.11 (wi-fi)标准。WEP使用[流密码RC4机密性](#)和[完整性的循环冗余Check-32](#) (CRC-32)校验和。

标准的64位WEP使用关键一个40的位(亦称WEP-40)，用24位初始化向量(iv)连接为了形成RC4密钥。一把64位WEP密钥通常被输入作为字符串10个十六进制(基础16)字符(零至九和A-F)。每个字符代表四个位，并且四个位十个位的每个等于40个位;如果添加24位IV，导致完整64位WEP密钥。

128-bit WEP密钥通常被输入作为26十六进制字符串。四个位二十六个位的每个个equals104位;如果添加24位IV，导致完整128-bit WEP密钥。多数设备允许用户输入密钥作为13个ASCII字符。

认证方法

两个验证方法可以与WEP一起使用：开放式系统验证和共享密钥认证。

使用开放式系统验证，WLAN客户端不需要提供凭证给AP为验证。所有客户端能验证与AP，然后尝试联合。实际上，验证不出现。随后，WEP密钥可以用于为了加密数据帧。这时，客户端必须有正确密钥。

使用共享密钥认证，WEP密钥使用验证在四步，质询响应握手：

1. 客户端向 AP 发送身份验证请求。
2. 与明文挑战的AP回复。
3. 客户端加密与已配置的WEP密钥的质询文本，并且回应另一认证请求。
4. AP解密答复。如果答复匹配质询文本，AP发送肯定回复。

在验证与关联以后，预共享WEP密钥也用于为了加密有RC4的数据帧。

在第一扫视，它也许似乎，好象共享密钥认证比开放式系统验证安全的更多，因为后者不提供实时验证。然而，反向是真的。如果捕获在共享密钥认证的质询帧派生用于握手keystream是可能的。因此，使用开放式系统验证WEP身份验证，而不是共享密钥认证是可行的。

临时密钥完整性协议(TKIP)创建为了解决这些WEP问题。类似于WEP，TKIP使用RC4加密。然而，TKIP提高WEP增加测量例如每个信息包密钥哈希算法，Message Integrity Check (MIC)和广播密钥交替为了针对已知WEP漏洞。TKIP以128-bit密钥加密和64位密钥使用RC4流密码验证。

配置

此部分为WEP提供GUI和CLI配置。

GUI 配置

完成这些步骤为了配置与GUI的WEP。

1. 连接对AP通过GUI。
2. 从在窗口的左边Security菜单，请选择您要配置您的静态WEP密钥的无线接口的加密管理器。
3. 在加密模式下，请点击WEP加密，并且选择必须从客户端的下拉菜单。

站点使用的加密模式是：

默认(不加密) -要求客户端通信与AP，不用任何数据加密。没有推荐此设置。**可选**-允许客户端通信与AP任一有或没有数据加密。一般，您使用此选项，当您有不能建立WEP联系时的客户端设备，例如非Cisco的客户端在128-bit WEP环境。**必须(完全加密)** -，当他们通信与AP时

，要求客户端使用数据加密。不使用数据加密的客户端没有允许通信。推荐此选项是否希望最大化您的WLAN安全。

4. 在加密密钥下，请选择**传送密钥**单选按钮，并且输入10位十六进制密钥。保证密钥大小设置为**40位**。

输入40位WEP密钥的10十六进制数字或者128-bit WEP密钥的26十六进制数字。密钥可以是这些位的所有组合：

0到9a到fA到F

5. 点击**全部应用**为了运用在两个的配置无线电。
6. 创建与**开放式验证**的一服务集标识(SSID)，并且单击**应用**为了启用它在两无线电。
7. 导航对网络，并且使**2.4 GHz**和**5 GHz**的无线电为了获得他们运行。

CLI 配置

请使用此部分为了配置与CLI的WEP。

```
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 $1$kxB1$0hRR4QtTUVDU9GakGDFs1
!
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

输入此命令为了确认您的配置适当地工作：

```
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](#)。

这些调试指令是有用的为了排除故障配置：

- **调试dot11事件**-启用所有dot1x事件的调试。
- **调试dot11数据包**-启用所有dot1x数据包的调试。

这是显示日志的示例，当客户端顺利地联合对WLAN：

```
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
```

当客户端输入错误的密钥时，此错误显示：

```
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
```