자동 액세스 포인트 컨피그레이션의 WEP 예

목차

소개

이 문서에서는 Cisco AP(Autonomous Access Point)에서 WEP(Wired Equivalent Privacy)를 사용하고 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 WLAN 디바이스에 대한 관리 연결을 설정할 수 있으며, 디바이스가 암호화되지 않은 환경에서 정상적으로 작동한다고 가정합니다. 표준 40비트 WEP를 구성하려면 서로 통신하는 무선 장치가 둘 이상 있어야 합니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS® Release15.2JB를 실행하는 1140 AP를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

WEP는 802.11(Wi-Fi) 표준에 내장된 암호화 알고리즘입니다. WEP는 기밀성을 위해 스트림 암호 RC4 를 사용하고 , 무결성을 위해 CRC-32(Cyclic Redundancy Check-32) 체크섬을 사용합니다!

표준 64비트 WEP는 RC4 키를 형성하기 위해 24비트 초기화 벡터 (IV)와 연결된 40비트 키(WEP-40이라고도 함)를 사용합니다. 64비트 WEP 키는 일반적으로 10개의 16진수(base 16) 문자(0~9 및 A-F)로 된 문자열로 입력됩니다. 각 문자는 4비트를 나타내며 4비트의 10자리 숫자는 각각 40비트입니다. 24비트 IV를 추가하면 완전한 64비트 WEP 키가 생성됩니다.

128비트 WEP 키는 일반적으로 26자의 16진수 문자열로 입력됩니다. 4비트의 26자리 숫자가 각각 104비트입니다. 24비트 IV를 추가하면 완전한 128비트 WEP 키가 생성됩니다. 대부분의 디바이스에서는 사용자가 키를 13자의 ASCII 문자로 입력할 수 있습니다.

인증 방법

WEP에서는 개방형 시스템 인증 및 공유 키 인증이라는 두 가지 인증 방법을 사용할 수 있습니다.

개방형 시스템 인증을 사용하면 WLAN 클라이언트가 인증을 위해 AP에 자격 증명을 제공할 필요가 없습니다. 모든 클라이언트는 AP를 통해 인증한 다음 연결을 시도할 수 있습니다. 사실상, 어떤 인증도 일어나지 않습니다. 그런 다음 WEP 키를 사용하여 데이터 프레임을 암호화할 수 있습니다. 이때 클라이언트는 올바른 키를 가져야 합니다.

공유 키 인증을 사용하는 경우 WEP 키는 다음과 같은 4단계 챌린지 응답 핸드셰이크의 인증에 사용됩니다.

1. 클라이언트는 AP에 인증 요청을 보냅니다.
2. AP가 일반 텍스트 챌린지로 응답합니다.
3. 클라이언트는 구성된 WEP 키로 챌린지 텍스트를 암호화하고 다른 인증 요청에 응답합니다.
4. AP가 응답의 암호를 해독합니다. 응답이 challenge-text와 일치하면 AP가 긍정적인 응답을 보냅니다.

인증 및 연결 후에는 사전 공유 WEP 키를 사용하여 RC4로 데이터 프레임을 암호화합니다.

언뜻 보기에 공유 키 인증은 개방형 시스템 인증보다 더 안전합니다. 개방형 시스템 인증은 실제 인증을 제공하지 않기 때문입니다. 그러나 그 반대는 사실이다. 공유 키 인증에서 챌린지 프레임을 캡처하는 경우 핸드셰이크에 사용되는 키 스트림을 파생시킬 수 있습니다. 따라서 WEP 인증에는 공유 키 인증 대신 개방형 시스템 인증을 사용하는 것이 좋습니다.

이러한 WEP 문제를 해결하기 위해 임시 키 통합 프로토콜(TKIP)이 생성되었습니다. WEP와 마찬가지로 TKIP는 RC4 암호화를 사용합니다. 그러나 TKIP는 알려진 WEP 취약성을 해결하기 위해 패킷별 키 해싱, MIC(Message Integrity Check), 브로드캐스트 키 순환과 같은 수단을 추가하여 WEP를 향상시킵니다. TKIP는 암호화에 128비트 키, 인증에 64비트 키가 포함된 RC4 스트림 암호를 사용합니다.

구성

이 섹션에서는 WEP에 대한 GUI 및 CLI 컨피그레이션을 제공합니다.

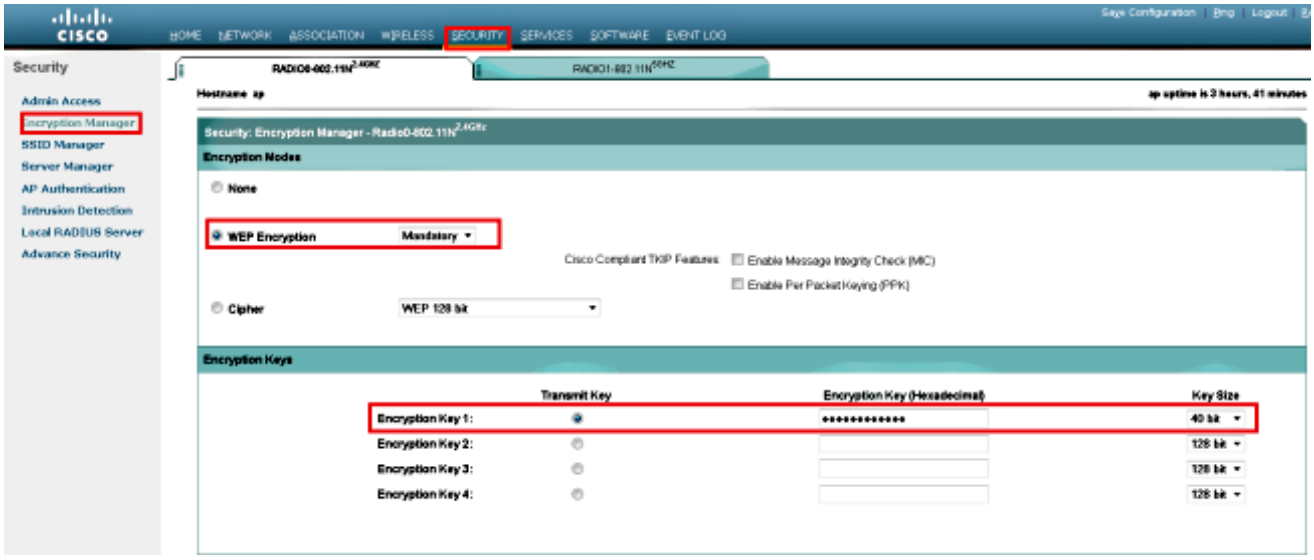
GUI 컨피그레이션

GUI를 사용하여 WEP를 구성하려면 다음 단계를 완료합니다.

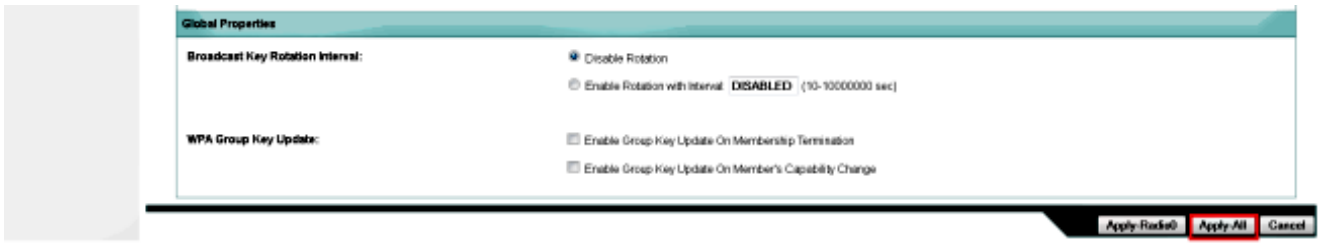
1. GUI를 통해 AP에 연결합니다.
2. 창의 왼쪽에 있는 보안 메뉴에서 고정 WEP 키를 구성하려는 무선 인터페이스에 대한 암호화 관리자를 선택합니다.
3. 암호화 모드에서 WEP 암호화를 클릭하고 클라이언트 드롭다운 메뉴에서 필수를 선택합니다.

   스테이션에서 사용하는 암호화 모드는 다음과 같습니다.
   - Default (No Encryption) - 클라이언트가 데이터 암호화 없이 AP와 통신해야 합니다. 이 설정은 권장되지 않습니다.
   - 선택 사항 - 클라이언트가 데이터 암호화를 사용하거나 사용하지 않고 AP와 통신할 수 있습니다. 일반적으로 128비트 WEP 환경의 비 Cisco 클라이언트와 같이 WEP 연결을 설정할 수 없는 클라이언트 장치가 있는 경우 이 옵션을 사용합니다.
   - 필수(전체 암호화) - 클라이언트가 AP와 통신할 때 데이터 암호화를 사용해야 합니다. 데이터 암호화를 사용하지 않는 클라이언트는 통신할 수 없습니다. WLAN의 보안을 극대화하려는 경우 이 옵션을 사용하는 것이 좋습니다.
4. Encryption Keys 아래에서 Transmit Key 라디오 버튼을 선택하고 10자리 16진수 키를 입력합니다. Key Size(키 크기)가 40비트로 설정되어 있는지 확인합니다.

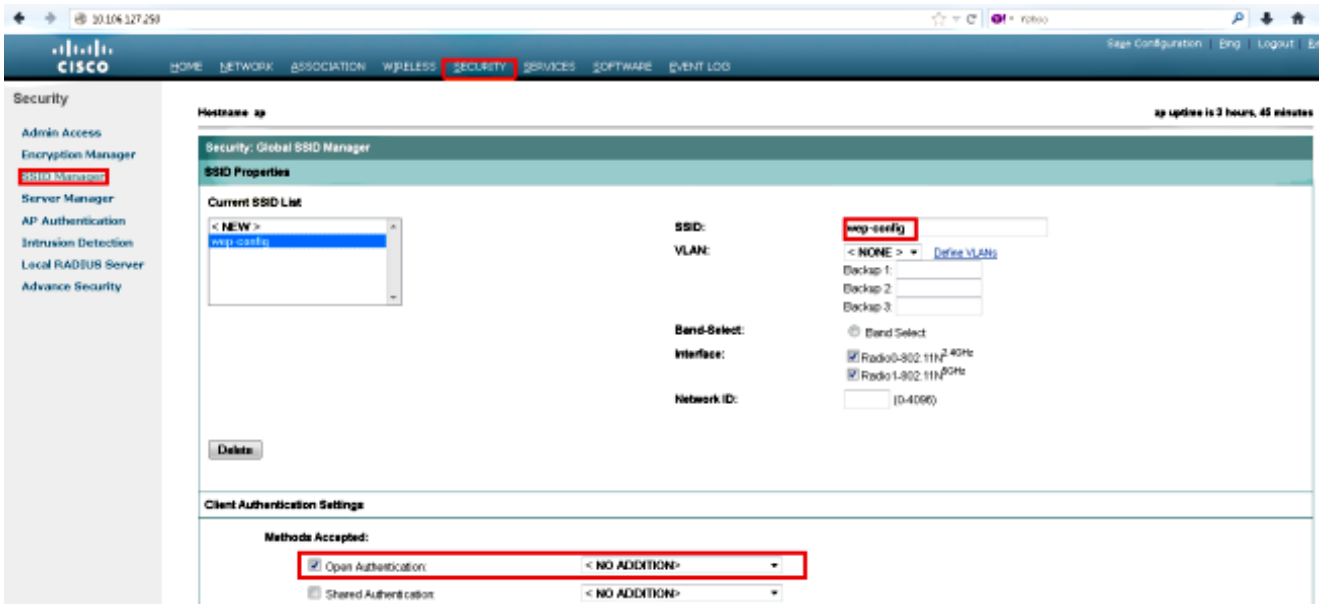
   40비트 WEP 키의 경우 10자리 16진수를 입력하고 128비트 WEP 키의 경우 26자리 16진수를 입력합니다. 키는 다음 숫자의 조합이 될 수 있습니다.
   - 0~9
   - a~f
   - A - F



5. Apply-All을 클릭하여 두 무선 장치에 컨피그레이션을 적용합니다.



6. 개방 인증을 사용하여 SSID(Service Set Identifier)를 생성하고 Apply(적용)를 클릭하여 두 무선 장치에서 모두 활성화합니다.



7. 네트워크를 탐색하고 2.4GHz 및 5GHz용 무선 장치를 활성화하여 실행합니다.

CLI 컨피그레이션

CLI를 사용하여 WEP를 구성하려면 이 섹션을 사용하십시오.

<#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
```

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 다음 명령을 입력합니다.

<#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
```

문제 해결

컨피그레이션 문제를 해결하려면 이 섹션을 사용합니다.

참고: debug 명령을 사용하기 전에 Debug 명령에 대한 중요 정보를 참조하십시오.

이러한 debug 명령은 컨피그레이션의 문제를 해결하는 데 유용합니다.

- debug dot11 events - 모든 dot1x 이벤트에 대한 디버그를 활성화합니다.
- debug dot11 packets - 모든 dot1x 패킷에 대한 디버그를 활성화합니다.

다음은 클라이언트가 WLAN에 성공적으로 연결할 때 표시되는 로그의 예입니다.

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

클라이언트가 잘못된 키를 입력하면 다음 오류가 표시됩니다.

```
*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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.