Aironet 액세스 포인트 및 브리지에 WEP 구성

목차

소개

이 문서에서는 Cisco Aironet Wireless LAN(WLAN) 구성 요소에 WEP(Wired Equivalent Privacy)를 구성하는 방법을 제공합니다.

참고: WLC(무선 LAN 컨트롤러)의 WEP 컨피그레이션에 대한 자세한 내용은 6장 - WLAN 구성의 정적 웹 키 섹션을 참조하십시오.

WEP는 802.11(Wi-Fi) 표준에 내장된 암호화 알고리즘입니다. WEP 암호화는 40비트 또는 104비트 키와 24비트 초기화 벡터(IV)가 있는 Ron의 코드 4(RC4) 스트림 암호를 사용합니다.

표준에서 지정한 대로 WEP는 40비트 또는 104비트 키와 24비트 IV가 있는 RC4 알고리즘을 사용합니다. RC4는 데이터의 암호화와 해독에 동일한 키를 사용하기 때문에 대칭 알고리즘입니다. WEP가 활성화되면 각 라디오 "스테이션"에 키가 있습니다. 이 키는 전파를 통해 데이터를 전송하기 전에 데이터를 스크램블하는 데 사용된다. 스테이션에서 적절한 키로 스크램블되지 않은 패킷을 수신하면 패킷은 폐기되고 호스트에 전달되지 않습니다.

WEP는 주로 홈 오피스 또는 매우 강력한 보안이 필요하지 않은 소규모 사무실에 사용될 수 있습니다.

하드웨어에 Aironet WEP 구현이 있습니다. 따라서 WEP를 사용할 때 성능에 미치는 영향이 최소화됩니다.

참고: WEP에 알려진 문제가 있어 강력한 암호화 방법이 아닙니다. 문제는 다음과 같습니다.

- 공유 WEP 키를 유지하는 데 많은 관리 오버헤드가 있습니다.
- WEP에는 공유 키를 기반으로 하는 모든 시스템과 동일한 문제가 있습니다. 한 사람에게 주어진 비밀은 일정 기간이 지나면 공개된다.
- WEP 알고리즘의 시드 IV는 일반 텍스트로 전송됩니다.
- WEP 체크섬은 선형 및 예측 가능합니다.

이러한 WEP 문제를 해결하기 위해 TKIP(임시 키 무결성 프로토콜)가 생성되었습니다. WEP와 마찬가지로 TKIP에서는 RC4 암호화를 사용합니다. 그러나 TKIP는 패킷별 키 해싱, MIC(Message Integrity Check), 브로드캐스트 키 회전 등의 조치를 추가하여 WEP의 알려진 취약성을 해결합니다. TKIP는 암호화에 128비트 키가 포함된 RC4 스트림 암호와 인증에 64비트 키를 사용합니다.

사전 요구 사항

요구 사항

이 문서에서는 WLAN 디바이스에 대한 관리 연결을 설정할 수 있으며 디바이스는 암호화되지 않은 환경에서 정상적으로 작동한다고 가정합니다.

표준 40비트 WEP를 구성하려면 서로 통신하는 두 개 이상의 무선 장치가 있어야 합니다.

참고: Aironet 제품은 IEEE 802.11b 호환 비Cisco 제품과 40비트 WEP 연결을 설정할 수 있습니다. 이 문서에서는 다른 디바이스의 컨피그레이션을 다루지 않습니다.

128비트 WEP 링크를 만들기 위해 Cisco 제품은 다른 Cisco 제품과의 상호 작용만 합니다.

사용되는 구성 요소

이 문서에서 다음 구성 요소를 사용합니다.

- 서로 통신하는 둘 이상의 라디오 장치
- WLAN 디바이스에 대한 관리 연결

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

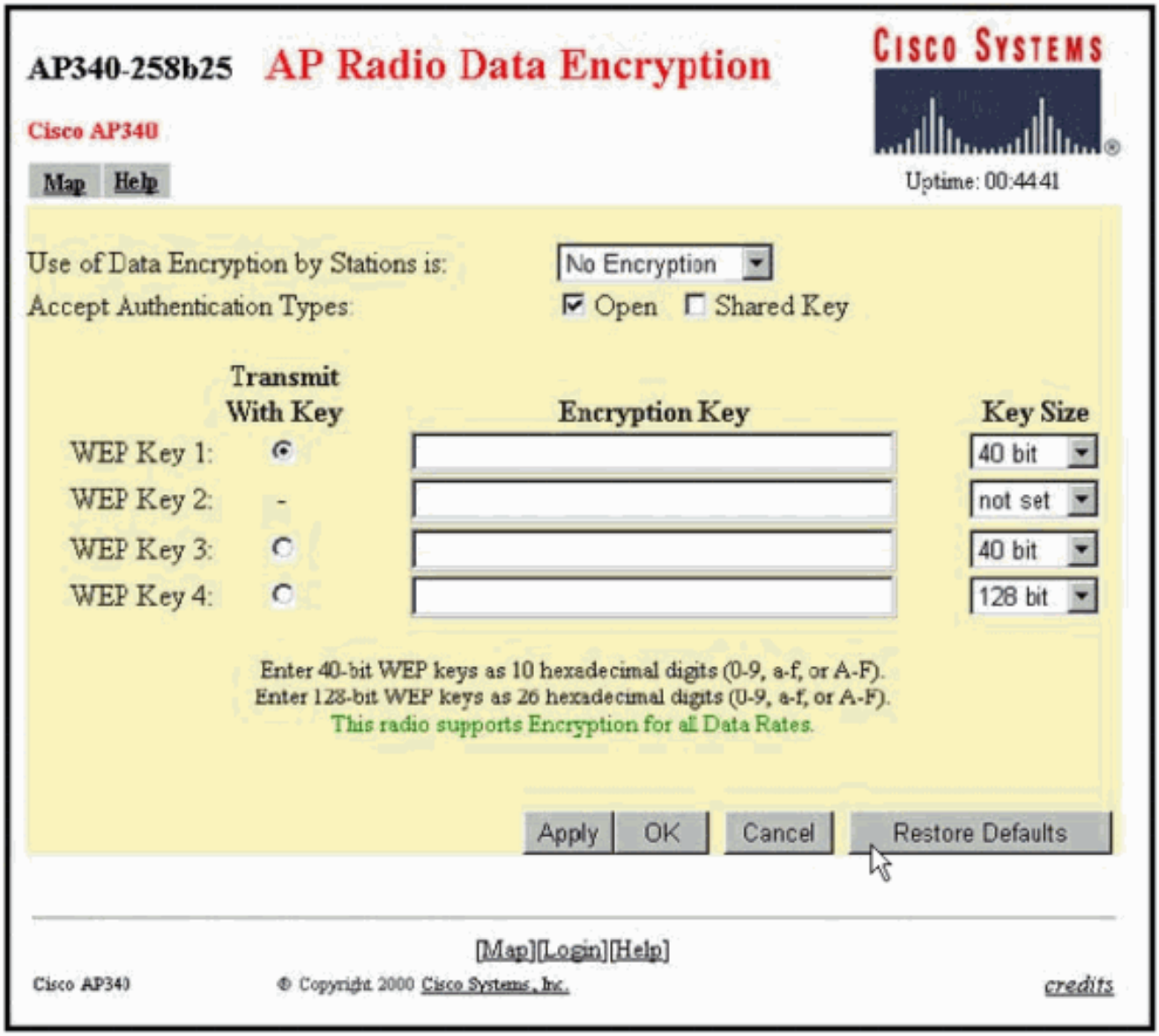
Aironet 액세스 포인트에서 WEP 구성

VxWorks 운영 체제를 실행하는 Aironet 액세스 포인트

다음 단계를 완료하십시오.

1. 액세스 포인트(AP)에 연결합니다.
2. AP Radio Encryption 메뉴로 이동합니다.다음 경로 중 하나를 사용합니다.**요약 상태 > 설정 >**

AP 라디오/하드웨어 > 무선 데이터 암호화(WEP) > AP 무선 데이터 암호화요약 상태 > 설정 > 보안 > 보안 설정: 무선 데이터 암호화(WEP) > AP 무선 데이터 암호화참고: 이 페이지를 변경하려면 ID 및 쓰기 기능을 가진 관리자여야 합니다.**AP 라디오 데이터 암호화 메뉴의 웹 브라우저 보기**



VxWorks 설정

AP Radio Data Encryption(AP 무선 데이터 암호화) 페이지는 다양한 사용 옵션을 제공합니다. 일부 옵션은 WEP에 필수적입니다. 이 섹션에서는 이러한 필수 옵션에 대해 설명합니다. WEP가 작동하려면 다른 옵션이 필요하지 않지만 권장됩니다.

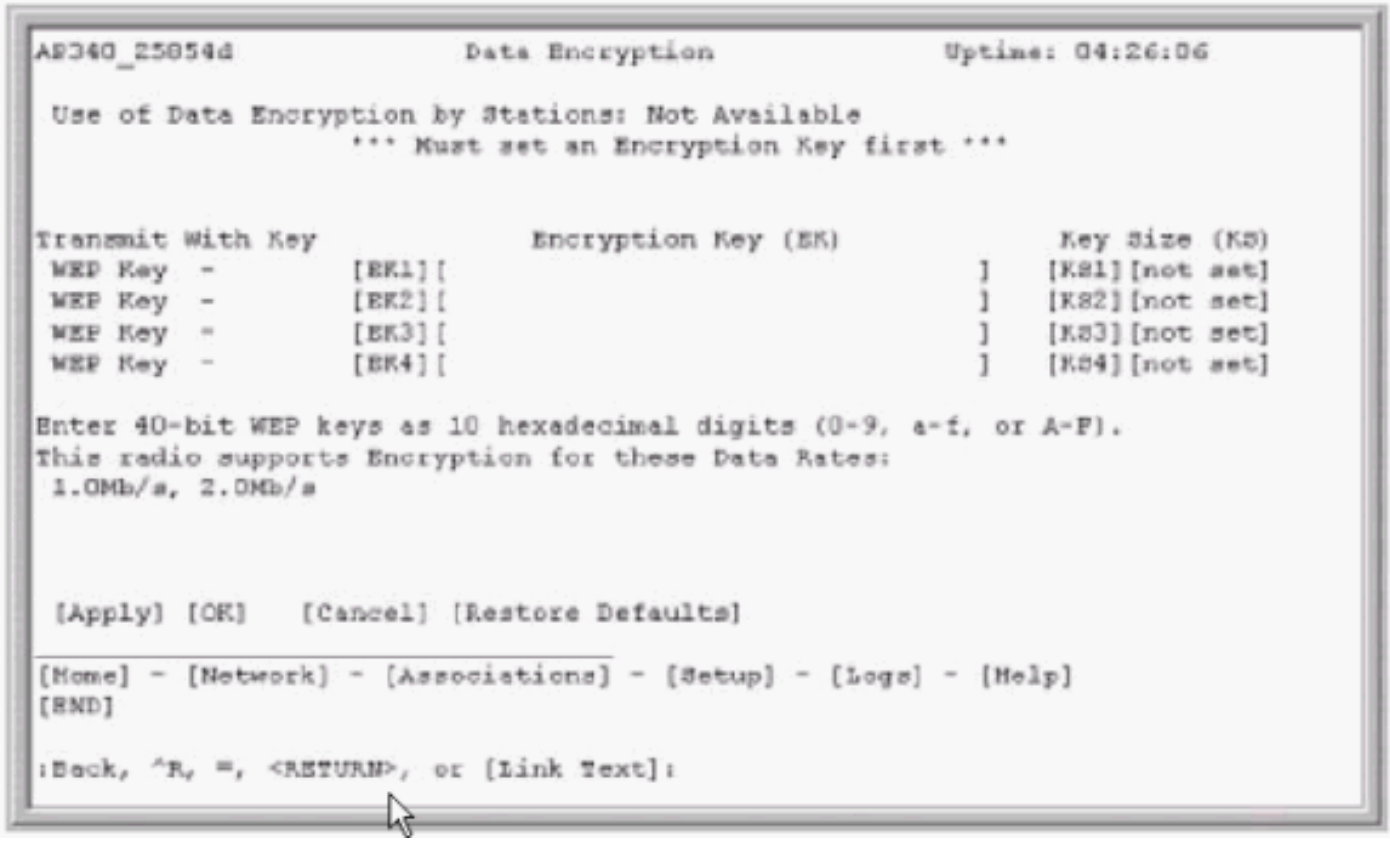
- **스테이션별 데이터 암호화 사용:**클라이언트가 AP와 통신할 때 데이터 암호화를 사용해야 하는지 여부를 선택하려면 이 설정을 사용합니다. 풀다운 메뉴에는 세 가지 옵션이 있습니다.**No Encryption(암호화 없음)(기본값)** - 클라이언트가 데이터 암호화 없이 AP와 통신해야 합니다. 이 설정은 권장되지 않습니다.**선택** 사항 - 클라이언트가 데이터 암호화를 사용하거나 사용하지 않고 AP와 통신할 수 있습니다. 일반적으로 128비트 WEP 환경에서 비 Cisco 클라이언트와 같이 WEP 연결을 만들 수 없는 클라이언트 장치가 있는 경우 이 옵션을 사용합니다.**Full Encryption (RECOMMENDED)(전체 암호화(RECOMMENDED)** - 클라이언트가 AP와 통신할 때 데이터 암호화를 사용해야 합니다. 데이터 암호화를 사용하지 않는 클라이언트는 통신할 수 없습니다. WLAN의 보안을 최대화하려는 경우 이 옵션을 사용하는 것이 좋습니다.**참고:** 암호화

사용을 활성화하려면 먼저 WEP 키를 설정해야 합니다. 이 목록의 **암호화 키(필수)** 섹션을 참조하십시오.

- **인증 유형 수락**AP에서 인식할 인증을 설정하려면 열기, 공유 키 또는 이 두 옵션 모두를 선택할 수 있습니다.**열기(권장)**—이 기본 설정은 WEP 키에 관계없이 모든 장치를 인증하고 연결을 시도할 수 있도록 합니다.**Shared Key(공유 키**) - 이 설정은 AP가 일반 텍스트 공유 키 쿼리를 AP와 연결하려고 시도하는 디바이스에 전송하도록 지시합니다.**참고:** 이 쿼리는 침입자의 알려진 텍스트 공격에 AP를 열어 둘 수 있습니다. 따라서 이 설정은 열기 설정만큼 안전하지 않습니다.
- **키를 사용하여 전송**이러한 단추를 사용하면 AP에서 데이터 전송 중에 사용하는 키를 선택할 수 있습니다. 한 번에 하나의 키만 선택할 수 있습니다. 세트 키 중 하나 또는 전체를 사용하여 데이터를 수신할 수 있습니다. 키를 Transmit Key로 지정하기 전에 설정해야 합니다.
- **암호화 키(필수)**이러한 필드를 사용하여 WEP 키를 입력할 수 있습니다. 40비트 WEP 키의 경우 10개의 16진수 숫자 또는 128비트 WEP 키의 경우 26개의 16진수 숫자를 입력합니다. 키는 다음 자릿수의 임의의 조합일 수 있습니다.0 ~ 90:00A ~ FWEP 키 보안을 보호하기 위해 기존 WEP 키는 입력 필드의 일반 텍스트에 나타나지 않습니다. 최신 버전의 AP에서는 기존 키를 삭제할 수 있습니다. 그러나 기존 키는 편집할 수 없습니다.**참고:** 네트워크, AP 및 클라이언트 장치에 대한 WEP 키를 동일하게 설정해야 합니다. 예를 들어 AP에서 WEP 키 3을 0987654321로 설정하고 이 키를 활성 키로 선택한 경우 클라이언트 장치의 WEP 키 3도 동일한 값으로 설정해야 합니다.
- **키 크기(필수)**이 설정은 키를 40비트 또는 128비트 WEP로 설정합니다. 이 선택에 대해 "설정되지 않음"이 나타나면 키가 설정되지 않습니다.**참고:** "설정되지 않음"을 선택하여 키를 삭제할 수 없습니다.
- **작업 단추**4개의 작업 단추가 설정을 제어합니다. 웹 브라우저에서 JavaScript를 사용할 수 있는 경우 Cancel(취소)을 제외한 임의의 버튼을 클릭하면 확인 팝업 창이 나타납니다.**적용**(Apply) - 새 값 설정을 활성화합니다. 브라우저가 페이지에 남아 있습니다.**확인** - 이 단추는 새 설정을 적용하고 브라우저를 기본 설정 페이지로 다시 이동합니다.**Cancel(취소**) - 이 단추는 설정 변경을 취소하고 이전에 저장된 값으로 설정을 반환합니다. 그런 다음 기본 설정 페이지로 돌아갑니다.**Restore Defaults(기본값 복원**) - 이 버튼을 클릭하면 이 페이지의 모든 설정이 공장 기본 설정으로 다시 변경됩니다.

참고: 최근 Cisco IOS® 버전의 AP에서는 이 페이지에 **Apply** 및 **Cancel** 컨트롤 버튼만 사용할 수 있습니다.

데이터 암호화 메뉴의 터미널 에뮬레이터 보기



WEP 키 구성 시퀀스의 터미널 에뮬레이터 보기(Cisco IOS® 소프트웨어)

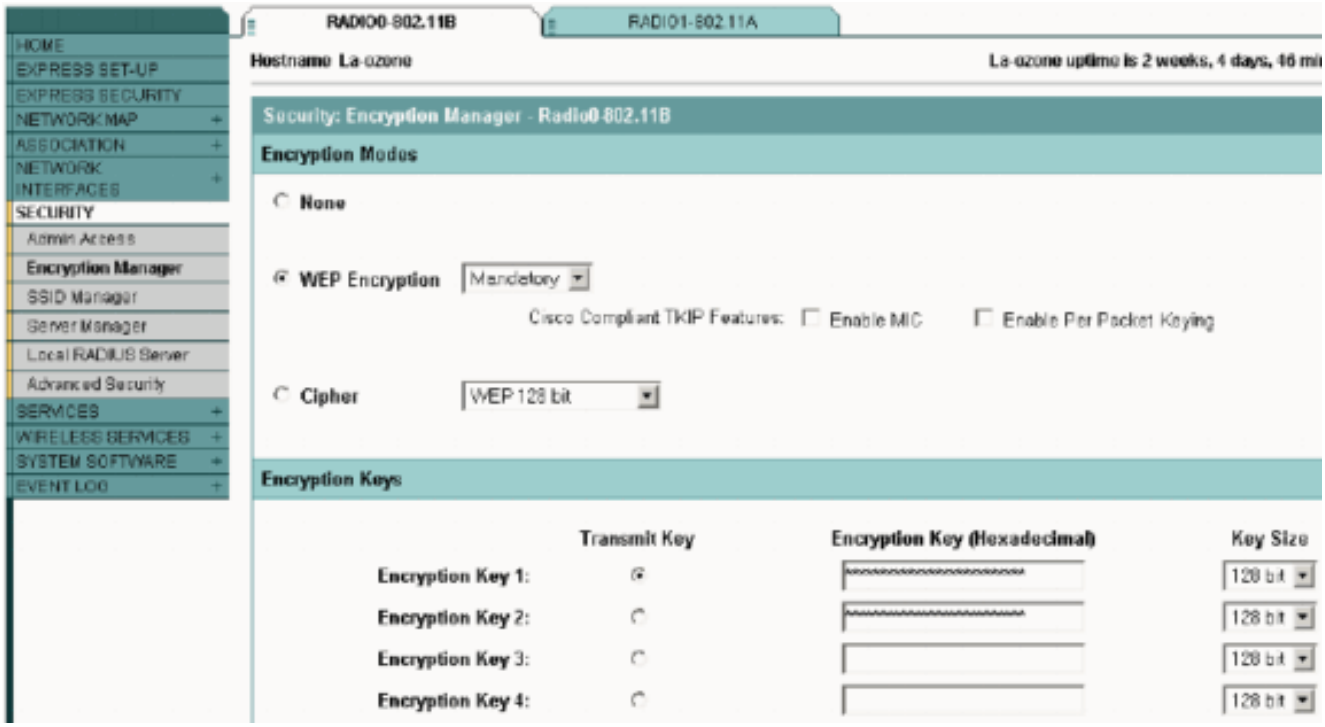
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
  transmit-key  Set the key as transmit key
  <cr>

La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee transmit-key
La-ozone(config-if)#end
La-ozone#
*Mar 19 00:42:13.893: %SYS-5-CONFIG_I: Configured from console by console
La-ozone#
La-ozone#
```

Cisco IOS 소프트웨어를 실행하는 Aironet AP

다음 단계를 완료하십시오.

1. AP에 연결합니다.
2. 창 왼쪽의 보안 메뉴 옵션에서 고정 WEP 키를 구성할 무선 인터페이스에 대해 **암호화 관리자**를 선택합니다.**AP Security Encryption Manager 메뉴의 웹 브라우저 보기**



Aironet 브리지 구성

VxWorks를 사용하는 경우 다음 단계를 완료합니다.

1. 브리지에 연결합니다.
2. 프라이버시 메뉴로 이동합니다.Main **Menu(기본 메뉴) > Configuration(구성) > Radio(라디오) > I80211 > Privacy(개인 정보)를 선택합니다**.Privacy(프라이버시) 메뉴는 무선에 의해 공중으로 전송되는 데이터 패킷에서 암호화 사용을 제어합니다. RSA RC4 알고리즘과 최대 4개의 알려진 키 중 하나를 사용하여 패킷을 암호화합니다. 라디오 셀의 각 노드는 사용 중인 모든 키를 알고 있어야 하지만, 데이터를 전송하기 위해 키를 선택할 수 있습니다.**개인 정보 메뉴의 터미널 에뮬레이터 보기**

```
        Configuration Radio I80211 Privacy Menu
     Option          Value       Description
1 - Encryption    [ off  ]    - Encrypt radio packets
2 - Auth          [ open ]    - Authentication mode
3 - Client        [ open ]    - Client authentication modes allowed
4 - Key                       - Set the keys
5 - Transmit                  - Key number for transmit
 Enter an option number or name, "=" main menu, <ESC> previous menu
>_
```

CLI 모드를 통한 1300 및 1400 Series 브리지의 WEP 구성 방법에 대한 자세한 내용은 암호 그룹 및 WEP - 1300 Series 브리지 및 WEP 기능 구성 - 1400 Series 브리지를 참조하십시오.

GUI를 사용하여 1300 및 1400 Series 브리지를 구성하려면 이 문서의 Cisco IOS Software를 실행하는 Aironet APs 섹션에 설명된 동일한 절차를 완료합니다.

VxWorks 설정

Privacy(프라이버시) 메뉴에는 구성해야 하는 옵션 집합이 표시됩니다. 일부 옵션은 WEP에 필수적입니다. 이 섹션에서는 이러한 필수 옵션에 대해 설명합니다. WEP가 작동하려면 다른 옵션이 필요

하지 않지만 권장됩니다.

이 섹션에서는 개인 정보 메뉴의 터미널 에뮬레이터 보기에 표시되는 순서대로 메뉴 옵션을 제공합니다. 그러나 다음 순서로 옵션을 구성합니다.

1. 키
2. 전송
3. 인증
4. 클라이언트
5. 암호화

이 순서대로 구성하면 각 설정을 구성할 때 필요한 전제 조건이 설정됩니다.

다음은 옵션입니다.

- **키(필수)**Key 옵션은 Bridge에 암호화 키를 프로그래밍합니다. 4개의 키 중 하나를 설정하라는 메시지가 표시됩니다. 키를 두 번 입력하라는 메시지가 표시됩니다. 키를 정의하려면 Bridge 컨피그레이션이 40비트 또는 128비트 키에 대한 것인지 여부에 따라 10 또는 26개의 16진수 숫자를 입력해야 합니다. 다음 숫자를 조합하여 사용합니다.0 ~ 90:00A ~ F키는 라디오 셀의 ***모든 노드***에서 일치해야 하며 동일한 순서로 키를 입력해야 합니다. WLAN의 각 디바이스에서 키 수가 일치하면 4개의 키를 모두 정의할 필요는 없습니다.
- **전송**Transmit 옵션은 패킷을 전송하기 위해 사용할 키를 라디오에 알려 줍니다. 각 무선 장치는 4개의 키 중 하나로 전송된 수신 패킷을 해독할 수 있습니다.
- **인증**리피터 브리지에서 Auth 옵션을 사용하여 유닛에서 어떤 인증 모드를 사용하여 상위 브리지 와 연결할지 결정할 수 있습니다. 허용되는 값은 Open 또는 Shared Key입니다. 802.11 프로토콜은 클라이언트가 연결할 수 있으려면 먼저 클라이언트가 상위를 인증해야 하는 절차를 지정합니다.**Open(RECOMMENDED)**—이 인증 모드는 기본적으로 null 작업입니다. 모든 클라이언트를 인증할 수 있습니다.**Shared Key(공유 키)** - 이 모드에서는 상위 사용자가 클라이언트에 챌린지 텍스트를 보낼 수 있습니다. 클라이언트는 이 텍스트를 암호화하여 상위 항목으로 돌아갑니다. 부모가 챌린지 텍스트를 성공적으로 해독하면 클라이언트가 인증됩니다.**주의:** 공유 키 모드를 사용하지 마십시오. 이를 사용하면 동일한 데이터의 일반 텍스트 및 암호화된 버전이 공중에서 전송됩니다. 이것은 아무 것도 얻지 못한다. 사용자 키가 잘못되면 유닛에서 패킷을 해독하지 않으며 패킷이 네트워크에 액세스할 수 없습니다.
- **클라이언트**Client 옵션은 클라이언트 노드가 장치에 연결하는 데 사용하는 인증 모드를 결정합니다. 허용되는 값은 다음과 같습니다.**Open(RECOMMENDED)**—이 인증 모드는 기본적으로 null 작업입니다. 모든 클라이언트를 인증할 수 있습니다.**Shared Key(공유 키)** - 이 모드에서는 상위 사용자가 클라이언트에 챌린지 텍스트를 보낼 수 있습니다. 클라이언트는 이 텍스트를 암호화하여 상위 항목으로 돌아갑니다. 부모가 챌린지 텍스트를 성공적으로 해독하면 클라이언트가 인증됩니다.**Both**(모두) - 이 모드에서는 클라이언트가 두 모드 중 하나를 사용할 수 있습니다.
- **암호화꺼짐**— Encryption 옵션을 Off로 설정하면 암호화가 수행되지 않습니다. 데이터는 암호화되지 않은 상태로 전송됩니다.**On(MANDATORY)**—Encryption(암호화) 옵션을 On(켜기)으로 설정하면 전송된 모든 데이터 패킷이 암호화되며 암호화되지 않은 수신 패킷은 삭제됩니다.**Mixed**(혼합) - Mixed(혼합) 모드에서 루트 또는 리피터 브리지는 암호화를 설정 또는 해제한 클라이언트의 연결을 수락합니다. 이 경우 두 지원 노드 간의 데이터 패킷만 암호화됩니다. 멀티캐스트 패킷은 암호화되지 않은 상태로 전송됩니다. 모든 노드는 패킷을 볼 수 있습니다.**주의:** 혼합 모드를 사용하지 마십시오. 암호화를 활성화한 클라이언트가 멀티캐스트 패킷을 해당 부모에 전송하는 경우 패킷이 암호화됩니다. 상위 는 패킷을 해독하고 암호화되지 않은 패킷을 셀에 재전송하며, 다른 노드는 패킷을 볼 수 있습니다. 암호화된 형식과 암호화되지 않은 형식으

로 패킷을 볼 수 있는 기능을 통해 키를 끊을 수 있습니다. 혼합 모드는 다른 벤더와의 호환성을 위해서만 포함됩니다.

클라이언트 어댑터 구성

Aironet 클라이언트 어댑터에 WEP를 설정하려면 다음 두 가지 기본 단계를 완료해야 합니다.

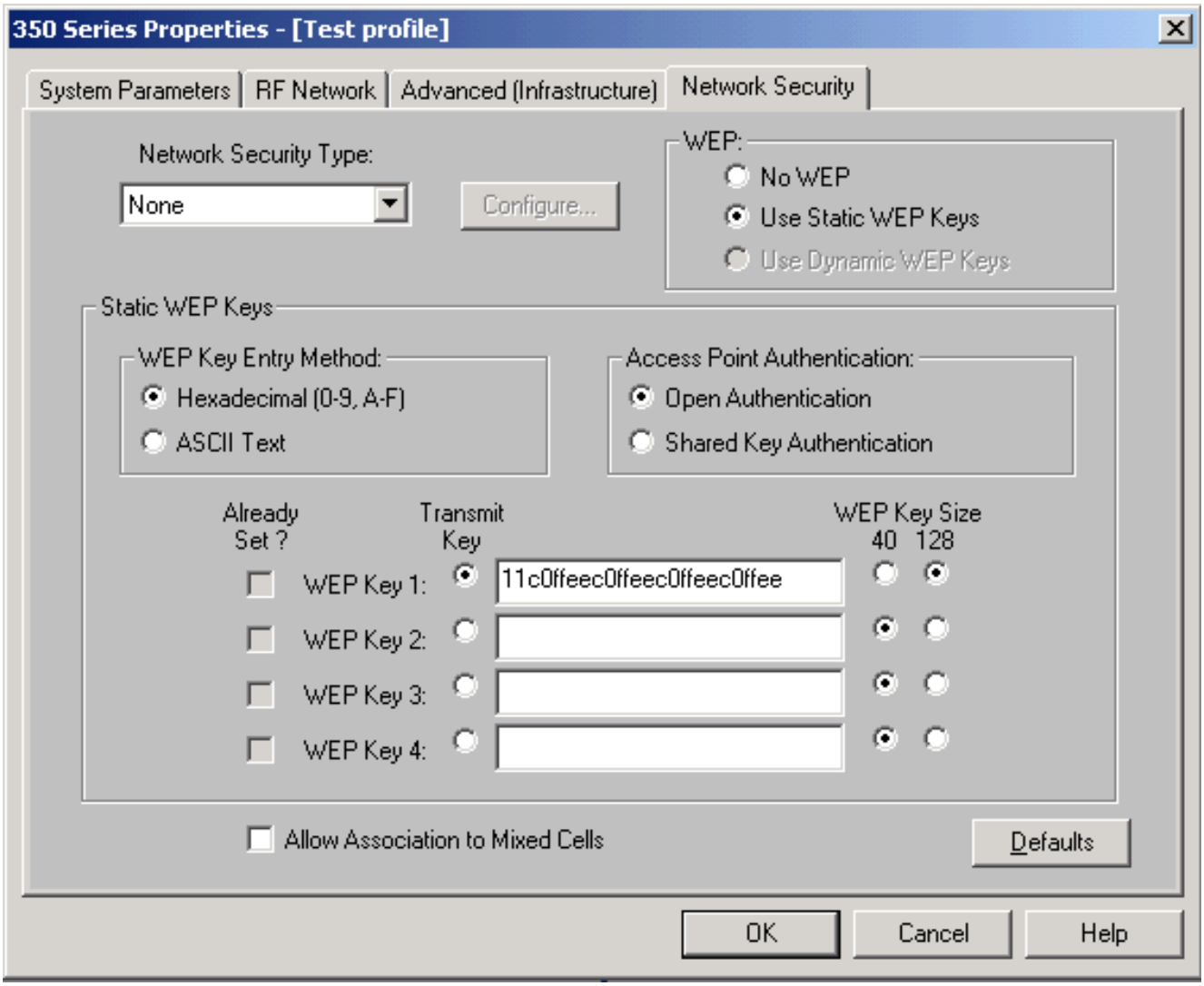
1. 클라이언트 암호화 관리자에서 WEP 키/키를 구성합니다.
2. ACU(Aironet Client Utility)에서 WEP를 활성화합니다.

WEP 키 설정

클라이언트 어댑터에 WEP 키를 설정하려면 다음 단계를 완료하십시오.

1. ACU를 열고 Profile **Manager를** 선택합니다.
2. WEP를 활성화할 프로파일을 선택하고 편집을 **클릭합니다**.
3. 보안 옵션을 표시하려면 **네트워크 보안** 탭을 클릭하고 고정 **WEP 키 사용을** 클릭합니다.이 작업은 WEP 없음을 선택하면 흐리게 표시되는 WEP 구성 옵션을 활성화합니다

.



4. 만들려는 WEP 키의 경우 창 오른쪽의 WEP 키 크기 아래에서 **40**비트 또는 **128**비트**를** 선택합니다.**참고:** 128비트 클라이언트 어댑터는 40비트 또는 128비트 키를 사용할 수 있습니다. 그러나 40비트 어댑터는 40비트 키만 사용할 수 있습니다.**참고:** 클라이언트 어댑터 WEP 키는

통신하는 다른 WLAN 구성 요소에서 사용하는 WEP 키와 일치해야 합니다.둘 이상의 WEP 키를 설정할 때 모든 장치에 대해 동일한 WEP 키 번호에 WEP 키를 할당해야 합니다. WEP 키는 16진수 문자로 구성되어야 하며 40비트 WEP 키의 경우 10자, 128비트 WEP 키의 경우 26자를 포함해야 합니다. 16진수 문자는 다음과 같을 수 있습니다.0 ~ 90:00A ~ F**참고:** ASCII-text WEP 키는 Aironet AP에서 지원되지 않습니다. 따라서 이러한 AP와 함께 클라이언트 어댑터를 사용하려는 경우 16진수(0-9, A-F) 옵션을 선택해야 합니다.**참고:** WEP 키를 만든 후 그 위에 쓸 수 있습니다. 그러나 편집하거나 삭제할 수는 없습니다.**참고:** ACU 대신 최신 버전의 Aironet Desktop Utility(ADU)를 클라이언트 유틸리티로 사용하는 경우 생성된 WEP 키를 삭제하고 새 키로 대체할 수도 있습니다.
5. 생성한 키 옆에 있는 Transmit Key 버튼을 클릭합니다.이 작업을 수행하면 이 키가 패킷을 전송하는 데 사용할 키임을 나타냅니다.
6. WEP 키 유형 아래에서 영구 를 클릭합니다.이 작업을 수행하면 어댑터 전원이 제거되거나 키가 설치된 컴퓨터를 재부팅하더라도 클라이언트 어댑터가 이 WEP 키를 유지할 수 있습니다. 이 옵션에 대해 Temporary(임시)를 선택하면 클라이언트 어댑터에서 전원이 분리되면 WEP 키가 손실됩니다.
7. **확인**을 **클릭합니다**.

WEP 사용

다음 단계를 완료하십시오.

1. ACU를 열고 메뉴 모음에서 **속성 편집**을 선택합니다.
2. 보안 옵션을 표시하려면 **네트워크 보안** 탭을 클릭합니다.
3. WEP를 **활성화하려면** WEP 사용 확인란을 선택합니다.

ADU를 클라이언트 유틸리티로 사용하여 WEP를 구성하는 단계는 ADU에서 WEP 구성을 참조하십시오.

워크그룹 브리지 구성

Aironet 340 Series Workgroup Bridge와 Aironet 340 Series Bridge는 서로 다릅니다. 그러나 WEP를 사용하기 위한 작업 그룹 브리지의 구성은 브리지 구성과 거의 동일합니다. 브리지의 컨피그레이션은 Aironet 브리지 구성 섹션을 참조하십시오.

1. 작업 그룹 브리지에 연결합니다.
2. 프라이버시 메뉴로 이동합니다.Privacy VxWorks 메뉴**에 액세스하려면 Main > Configuration > Radio > I80211 > Privacy**를 선택합니다.

설정

프라이버시 메뉴에는 이 섹션에 나열되는 설정이 표시됩니다. 다음 순서로 작업 그룹 브리지에 옵션을 구성합니다.

1. 키
2. 전송
3. 인증
4. 암호화

다음은 옵션입니다.

- **키**키 옵션은 패킷을 받기 위해 브리지에서 사용하는 WEP 키를 설정합니다. 이 값은 작업 그룹 브리지가 통신하는 AP 또는 다른 장치에서 사용하는 키와 일치해야 합니다. 키는 40비트 암호화에 대해 최대 10개의 16진수 문자 또는 128비트 암호화에 대해 26개의 16진수 문자로 구성됩니다. 16진수 문자는 다음 자릿수를 조합하여 사용할 수 있습니다.0 ~ 90:00A ~ F
- **전송**전송 옵션은 패킷을 전송하기 위해 브리지에서 사용하는 WEP 키를 설정합니다. 키 옵션에 사용한 것과 동일한 키를 사용하도록 선택할 수 있습니다. 다른 키를 선택하는 경우 AP에서 일치하는 키를 설정해야 합니다.한 번에 하나의 WEP 키만 전송에 사용할 수 있습니다. 데이터를 전송하는 데 사용하는 WEP 키는 작업 그룹 브리지 및 이 장치가 통신하는 다른 장치에서 동일한 값으로 설정해야 합니다.
- **인증(인증)**Auth 매개 변수는 시스템에서 사용하는 인증 방법을 결정합니다. 옵션은 다음과 같습니다.**열기(권장)**—기본 열기 설정을 사용하면 WEP 설정에 관계없이 모든 AP가 인증되고 브리지와 통신을 시도할 수 있습니다.**Shared Key(공유 키)** - 이 설정은 브리지와 통신을 시도하여 AP에 일반 텍스트 공유 키 쿼리를 전송하도록 브리지에 지시합니다. 공유 키 설정은 침입자의 알려진 텍스트 공격에 브리지를 열어 둘 수 있습니다. 따라서 이 설정은 열기 설정만큼 안전하지 않습니다.
- **암호화**Encryption 옵션은 연결 패킷 및 일부 제어 패킷을 제외한 모든 데이터 패킷에 암호화 매개변수를 설정합니다. 4가지 옵션이 있습니다.**참고:** AP는 암호화를 활성화하고 키가 올바르게 설정되어야 합니다.**Off**(끄기) - 기본 설정입니다. 모든 암호화가 꺼져 있습니다. 작업 그룹 브리지는 WEP를 사용하여 AP와 통신하지 않습니다.**On(RECOMMENDED)** - 이 설정을 사용하려면 모든 데이터 전송을 암호화해야 합니다. 워크그룹 브리지는 WEP를 사용하는 AP와 통신만 합니다.**혼합**—이 설정은 브리지가 AP와 통신하기 위해 항상 WEP를 사용함을 의미합니다. 그러나 AP는 WEP를 사용하든 WEP를 사용하지 않든 모든 장치와 통신합니다.**혼합**—이 설정은 브리지가 AP와 통신하기 위해 WEP를 사용하지 않음을 의미합니다. 그러나 AP는 WEP를 사용하든 WEP를 사용하지 않든 모든 장치와 통신합니다.**주의:** WEP 범주로 켜짐 또는 혼합을 선택하고 라디오 링크를 통해 브리지를 구성하면 WEP 키를 잘못 설정하면 브리지에 대한 연결이 끊어집니다. 작업 그룹 브리지에서 WEP 키를 설정하고 WLAN의 다른 장치에서 WEP 키를 설정할 때 동일한 설정을 사용해야 합니다.

관련 정보

- IEEE 표준 연결
- Aironet 340 Series Wireless LAN 제품
- 무선 지원 리소스
- 무선 LAN 지원 페이지
- Cisco Aironet Access Point용 Cisco IOS 소프트웨어 구성 설명서
- Cisco Aironet 1300 Series Outdoor Access Point/Bridge용 Cisco IOS 소프트웨어 구성 설명서
- VxWorks용 Cisco Aironet Access Point Software 구성 설명서
- Cisco Aironet 1400 Series Bridge 소프트웨어 컨피그레이션 가이드
- Cisco Aironet Wireless LAN Client Adapters 컨피그레이션 가이드
- Cisco Wireless LAN Security 개요
- 무선(모빌리티) 무선 네트워크 보안
- 액세스 포인트를 작업 그룹 브리지 구성 예
- Cisco Aironet 워크그룹 브리지 FAQ
- Cisco Aironet 장비의 비밀번호 복구 절차
- Cisco Aironet 액세스 포인트 FAQ
- 기술 지원 및 문서 – Cisco Systems