통합 무선 네트워크에서 비인가 탐지

목차

소개

무선 네트워크는 유선 네트워크를 확장하며 직원의 생산성과 정보 액세스를 향상시킵니다. 그러나 무단 무선 네트워크는 추가적인 보안 문제를 야기합니다. 유선 네트워크에서는 포트 보안에 대한 인식이 줄어들고, 무선 네트워크는 유선 네트워크로 쉽게 확장됩니다. 따라서 자신의 Cisco AP(Access Point)를 안전한 무선 또는 유선 인프라에 가져오고 권한이 없는 사용자가 이 보안 네트워크에 액세스할 수 있도록 허용하는 직원은 보안 네트워크를 쉽게 감염시킬 수 있습니다.

비인가 탐지를 통해 네트워크 관리자는 이러한 보안 문제를 모니터링하고 제거할 수 있습니다. Cisco Unified Network Architecture는 오버레이 네트워크 및 툴에 대한 비용과 타당성을 입증하기 어려운 필요 없이 완전한 비인가 식별 및 억제 솔루션을 지원하는 두 가지 비인가 탐지 방법을 제공합니다.

기능 개요

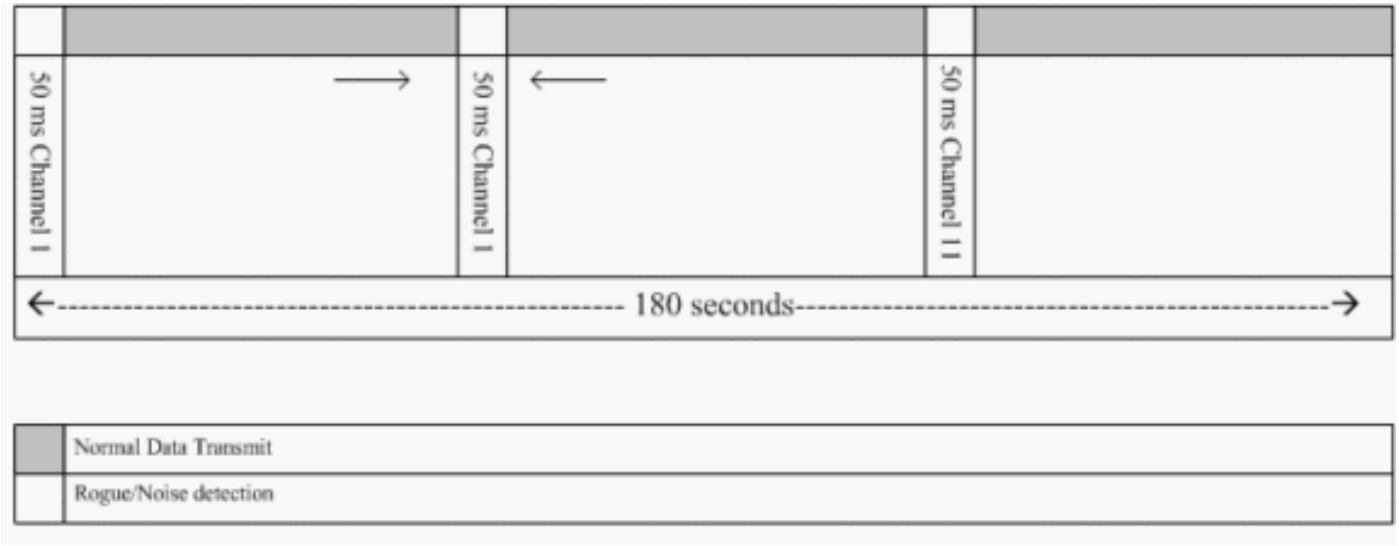
비인가 탐지는 어떤 규정에도 구속되지 않으며, 운영을 위해 법적 준수가 필요하지 않습니다. 그러나 비인가 억제는 일반적으로 인프라 공급업체가 자동으로 운영되도록 방치할 경우 불편할 수 있는 법적 문제를 야기합니다. Cisco는 이러한 문제에 매우 민감하며 이러한 솔루션을 제공합니다. 각 컨트롤러는 RF 그룹 이름으로 구성됩니다.경량 AP가 컨트롤러에 등록되면 모든 신호/프로브 응답 프레임에 컨트롤러에 구성된 RF 그룹에 특정한 **IE(Authentication Information Element)**를 포함합니다. 경량 AP가 이 **IE**가 없거나 **잘못된 IE**가 있는 AP에서 신호/프로브 응답 프레임을 들을 경우, 경량 AP는 AP를 비인가(Rogue)로 보고하고, 해당 BSSID를 비인가 테이블에 기록한 다음 테이블을 컨트롤러에 전송합니다. 두 가지 방법, 즉 RLDP(Rogue Location Discovery Protocol)와 패시브 작업이 있으며, 이 방법은 자세히 설명되어 있습니다. Determine Active Rogues 섹션을 참조하십시오.

인프라 비인가 검색

활성 무선 환경에서 비인가 검색을 수행하는 데 많은 비용이 들 수 있습니다. 이 프로세스에서는 서

비스 중인 AP(또는 로컬 모드)에 서비스 중지, 노이즈 수신, 비인가 탐지를 수행하도록 요청합니다. 네트워크 관리자는 스캔할 채널을 구성하고 모든 스테이션이 스캔되는 기간을 구성합니다. AP는 비인가 클라이언트 신호를 50ms를 수신한 다음 구성된 채널로 돌아와 클라이언트를 다시 서비스합니다. 이 활성 스캐닝은 네이버 메시지와 결합되어 어떤 AP가 비인가, 어떤 AP가 유효하고 네트워크의 일부인지 식별합니다. 스캔된 채널 및 검사 기간을 구성하려면 **Wireless > 802.11b/g Network**(네트워크 요구 사항에 따라 "**b/g**" 또는 "**a**")로 이동하고 브라우저 창 오른쪽 상단 모서리에서 Auto RF(자동 RF) 버튼을 선택합니다.

아래로 스크롤하여 **Noise/Interference/Rogue Monitoring Channels**로 이동하여 비인가 및 노이즈를 스캔할 채널을 구성할 수 있습니다. 사용 가능한 옵션은 다음과 같습니다. 모든 채널(1~14), 국가 채널(1~11) 또는 DCA(Dynamic Channel Association) 채널(기본값 1, 6, 11). 이러한 채널을 통한 스캐닝 기간은 노이즈 측정 간격과 함께 **Monitor Intervals(60~3600초)**에서 동일한 창에서 구성할 수 있습니다. 기본적으로 오프채널 노이즈 및 비거에 대한 수신 대기 간격은 180초입니다. 즉, 각 채널은 180초마다 스캔됩니다. 다음은 180초마다 스캔되는 DCA 채널의 예입니다.



예를 들어, 스캔하도록 구성된 많은 채널이 짧은 스캐닝 간격과 결합되어 AP가 실제로 데이터 클라이언트를 서비스할 시간이 줄어듭니다.

경량 AP는 클라이언트 및 AP에 비인가 레이블을 지정하기 위해 기다립니다. 다른 주기가 완료될 때까지 다른 AP에서 이러한 비인가가 보고되지 않을 수 있기 때문입니다. 동일한 AP가 동일한 채널로 다시 이동하여 비인가 AP와 클라이언트, 노이즈 및 간섭을 모니터링합니다. 동일한 클라이언트 및/또는 AP가 탐지되면 컨트롤러에 다시 비인가 상태로 나열됩니다. 이제 컨트롤러는 이러한 비인가가 로컬 네트워크에 연결되었는지 아니면 단순히 인접한 AP에 연결되었는지 확인하기 시작합니다. 어떤 경우든 매니지드 로컬 무선 네트워크에 속하지 않은 AP는 비인가(rogue)로 간주됩니다.

비인가 세부사항

경량 AP는 비인가 클라이언트를 듣고 노이즈 및 채널 간섭을 모니터링하기 위해 50ms 동안 오프채널로 이동합니다. 탐지된 모든 비인가 클라이언트 또는 AP가 컨트롤러로 전송되며, 컨트롤러는 다음 정보를 수집합니다.

- 비인가 AP MAC 주소
- 비인가 AP 이름
- 비인가 연결 클라이언트 MAC 주소
- 프레임이 WPA 또는 WEP로 보호되는지 여부
- 프리앰블
- SNR(Signal-to-Noise Ratio)

- 수신기 신호 강도 표시기(RSSI)

비인가 탐지기 액세스 포인트

AP를 비인가 탐지기(rogue detector)로 작동시킬 수 있습니다. 그러면 트렁크 포트에 배치하여 유선 측 연결 VLAN을 모두 들을 수 있습니다. 모든 VLAN의 유선 서브넷에서 클라이언트를 찾습니다. 비인가 탐지기 AP는 ARP(Address Resolution Protocol) 패킷을 수신하여 컨트롤러에서 전송하는 식별된 비인가 클라이언트 또는 비인가 AP의 레이어 2 주소를 확인합니다. 일치하는 레이어 2 주소가 발견되면 컨트롤러는 비인가 AP 또는 클라이언트를 위협으로 식별하는 경보를 생성합니다. 이 경보는 비가가 유선 네트워크에서 발견되었음을 나타냅니다.

활성 비인가 확인

비인가 AP는 컨트롤러에서 비인가 AP로 추가되기 전에 "두 번 확인"해야 합니다. 비인가 AP는 기업 네트워크의 유선 세그먼트에 연결되지 않은 경우 위협으로 간주되지 않습니다. 비가가 활성 상태인지 확인하기 위해 다양한 접근 방식이 사용됩니다. 이러한 접근 방식에는 RLDP가 포함됩니다.

RLDP(Rogue Location Discovery Protocol)

RLDP는 활성 접근 방식이며, 비인가 AP에 인증(Open Authentication)이 구성되지 않은 경우 사용됩니다. 기본적으로 비활성화된 이 모드는 활성 AP가 비인가 채널로 이동하고 비인가 채널에 클라이언트로 연결하도록 지시합니다. 이 시간 동안 활성 AP는 연결된 모든 클라이언트에 인증 해제 메시지를 전송한 다음 라디오 인터페이스를 종료합니다. 그런 다음 비인가 AP에 클라이언트로 연결됩니다.

그런 다음 AP는 비인가 AP에서 IP 주소를 얻으려고 시도하며, 비인가 AP를 통해 로컬 AP와 비인가 연결 정보가 포함된 UDP(User Datagram Protocol) 패킷(포트 6352)을 컨트롤러에 전달합니다. 컨트롤러가 이 패킷을 수신하면 RLDP 기능을 사용하여 유선 네트워크에서 비인가 AP가 발견되었음을 네트워크 관리자에게 알리도록 경보가 설정됩니다.

참고: Lightweight **AP가** 비인가 AP에서 DHCP 주소를 연결하고 수신하는지 확인하려면 debug dot11 rldp enable 명령을 사용합니다. 이 명령은 경량 AP에서 컨트롤러에 보낸 UDP 패킷도 표시합니다.

다음은 경량형 AP에서 보낸 UDP(목적지 포트 6352) 패킷의 예입니다.

```
0020 0a 01 01 0d 0a 01.......(.*..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00
000...x......... 0040 00 00 00 00 00 00 00 00 00 00 00 00
```

데이터의 처음 5바이트에는 비인가 AP가 로컬 모드 AP에 제공한 DHCP 주소가 포함됩니다. 다음 5바이트는 컨트롤러의 IP 주소이며, 그 뒤에 비인가 AP MAC 주소를 나타내는 6바이트가 옵니다. 그리고 18바이트의 0이 있습니다.

수동 작업:

이 접근 방식은 비인가 AP에 WEP 또는 WPA와 같은 인증 형식이 있을 때 사용됩니다. 비인가 AP에 인증 형식이 구성된 경우 비인가 AP에 구성된 키를 알지 못하므로 경량형 AP를 연결할 수 없습니다. 비인가 클라이언트 MAC 주소 목록에 있는 컨트롤러가 비인가 탐지기로 구성된 AP로 전달되면 이 프로세스는 컨트롤러로 시작됩니다. 비인가 탐지기는 연결된 모든 서브넷에서 ARP 요청을 스캔하며, ARP는 일치하는 레이어 2 주소를 검색합니다. 일치하는 항목이 검색되면 컨트롤러는 네트워크 관리자에게 비거가 유선 서브넷에서 탐지되었음을 알립니다.

활성 비인가 억제

유선 네트워크에서 비인가 클라이언트가 탐지되면 네트워크 관리자는 비인가 AP와 비인가 클라이언트를 모두 포함할 수 있습니다. 이 작업은 802.11 비인가 AP와 연결된 클라이언트로 802.11 비인증 패킷을 전송하여 이러한 구멍에서 생성되는 위협을 완화하므로 가능합니다. 비인가 AP를 억제하려는 시도가 있을 때마다 경량 AP 리소스의 약 15%가 사용됩니다. 따라서 비인가 AP가 포함된 후에는 이를 물리적으로 찾아 제거하는 것이 좋습니다.

참고: WLC 릴리스 5.2.157.0에서 루즈가 탐지되면 이제 탐지된 비가를 수동으로 또는 자동으로 포함할지 선택할 수 있습니다. 5.2.157.0 이전 컨트롤러 소프트웨어 릴리스에서는 수동 컨테인먼트가 유일한 옵션입니다.

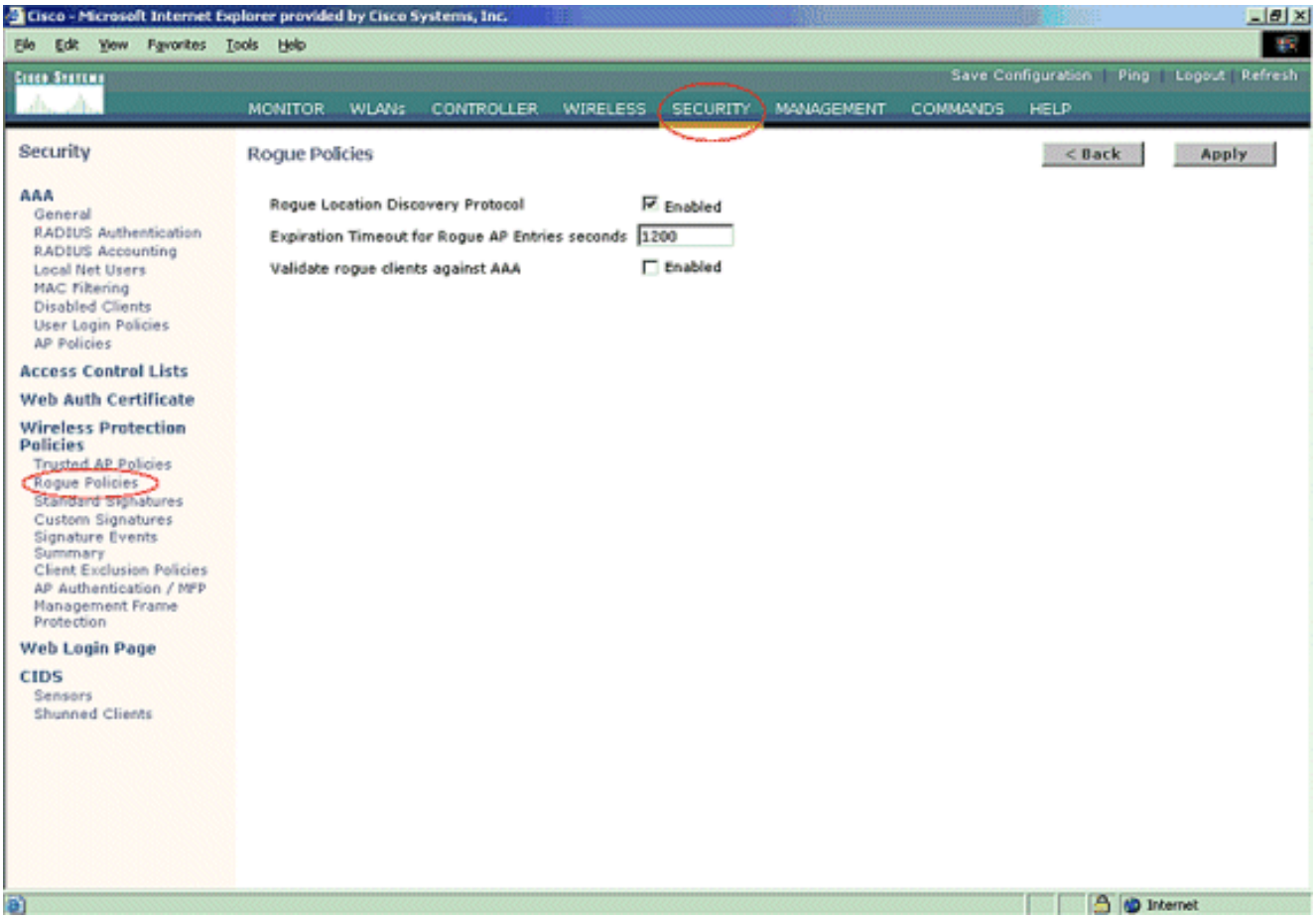
비인가 탐지 - 컨피그레이션 단계

거의 모든 비인가 탐지 컨피그레이션은 기본적으로 활성화되어 즉시 사용 가능한 최대화된 네트워크 보안을 제공합니다. 이러한 컨피그레이션 단계에서는 중요한 비인가 탐지 정보를 명확하게 하기 위해 컨트롤러에 비인가 탐지가 설정되지 않았다고 가정합니다.

비인가 탐지를 설정하려면 다음 단계를 완료하십시오.

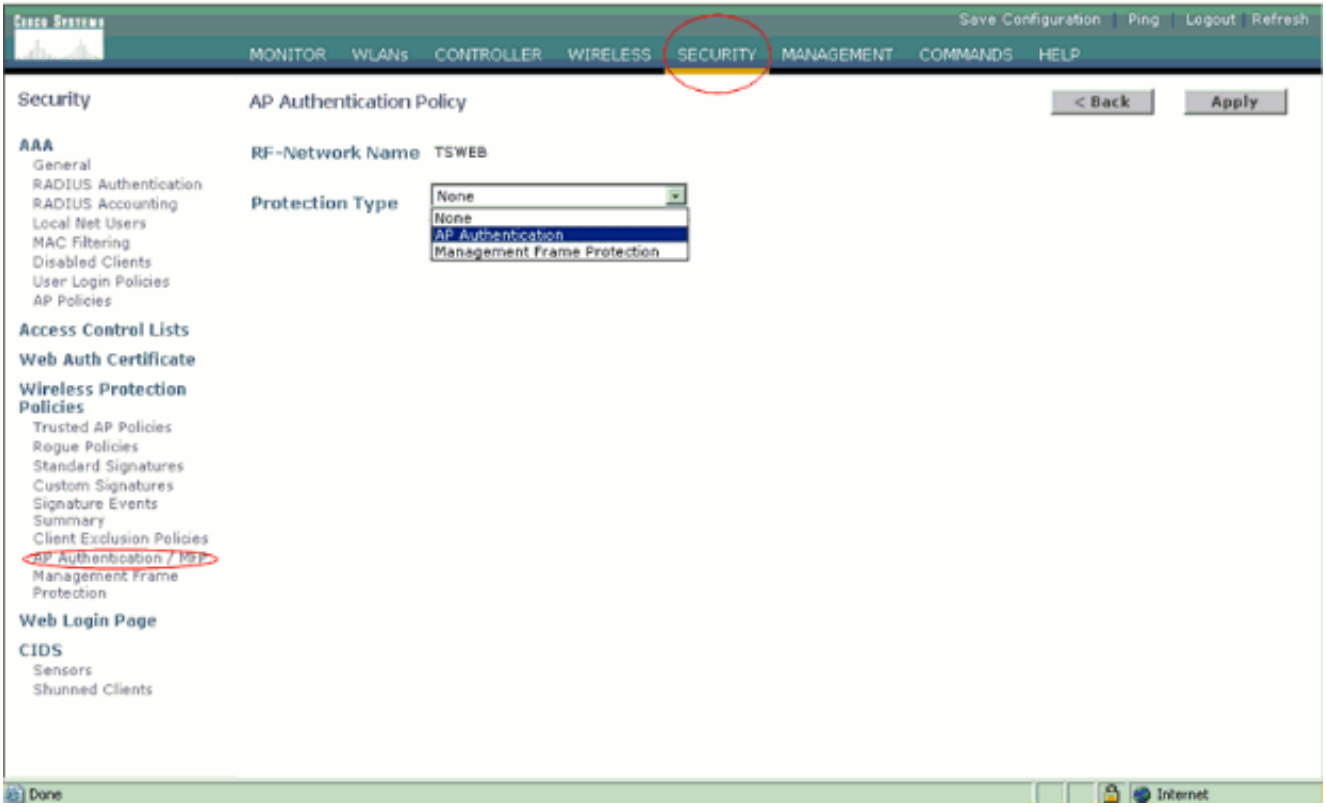
1. 비인가 위치 검색 프로토콜이 켜져 있는지 확인합니다. 이 기능을 켜려면 그림에 표시된 대로 **Security(보안) > Rogue Policies(비인가 정책)**를 선택하고 **Enabled**(비인가 위치 **검색 프로토콜**)에서 Enabled(활성화됨)를 클릭합니다.**참고:** 비인가 AP가 일정 시간 동안 들리지 않으면 컨트롤러에서 제거됩니다. 이는 **비인가** AP에 대한 만료 시간 제한이며, 이는 RLDP 옵션 아래에 구성됩니다

.



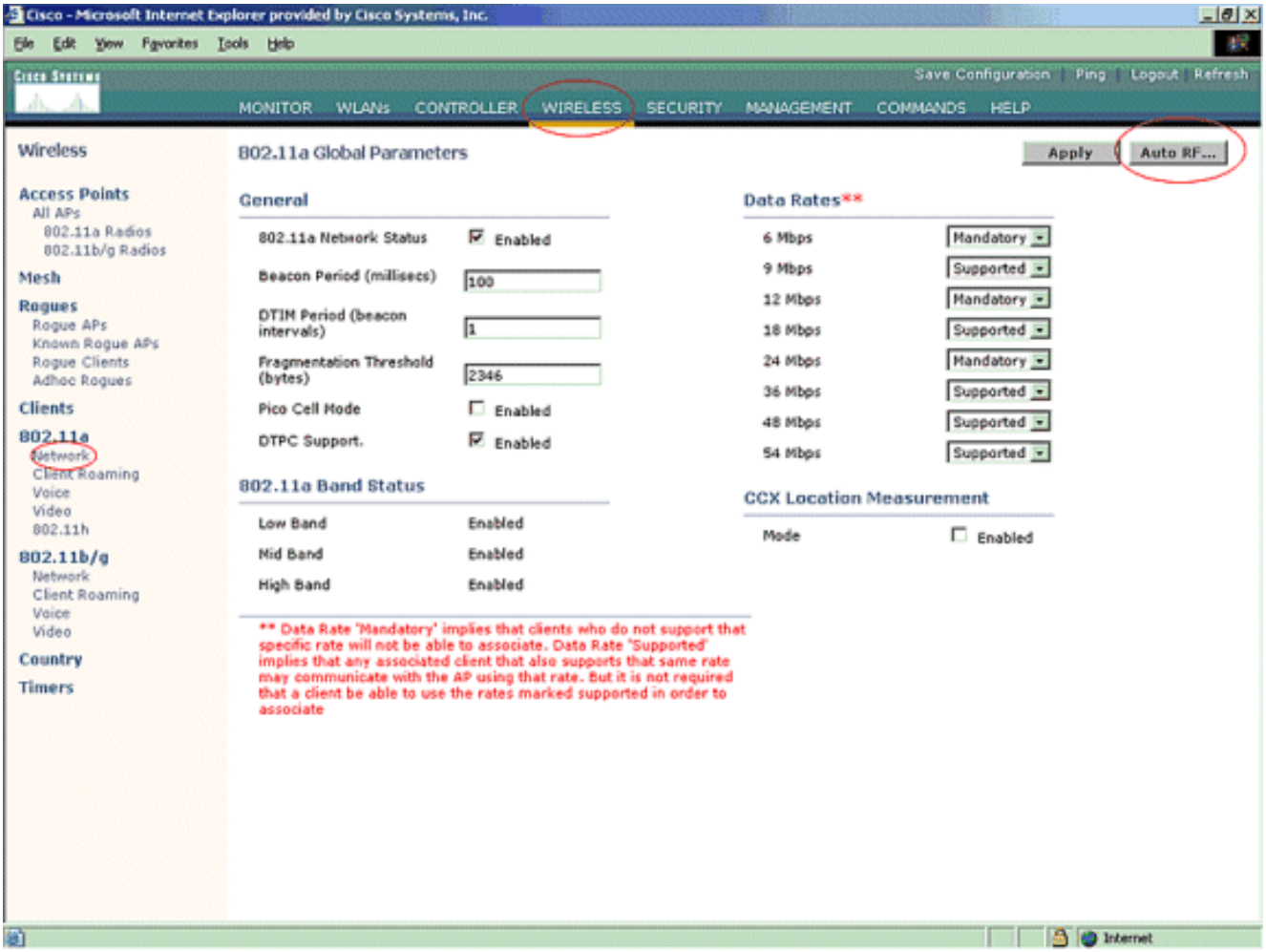
2. 이 단계는 선택 사항입니다. 이 기능을 활성화하면 RF **그룹** 이름이 다른 RF 네이버 패킷을 전송하는 AP가 비인가로 보고됩니다. 이는 RF 환경 연구에 도움이 됩니다. 활성화하려면 Security(보안) **-> AP Authentication(AP 인증)을** 선택합니다. 그런 다음 **AP Authentication(AP 인증)**을 그림에 표시된 보호 유형으로 선택합니다

.



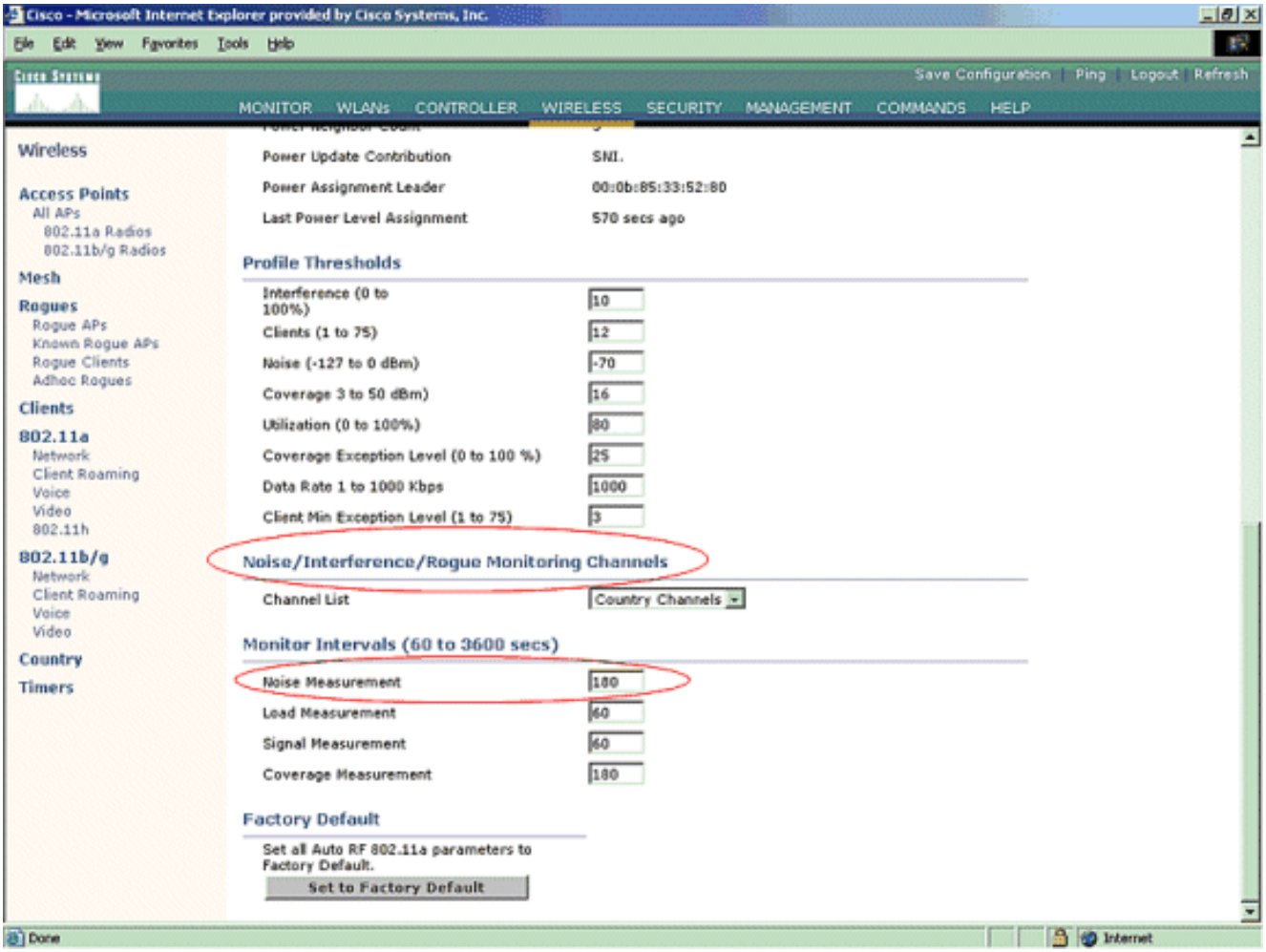
3. 다음 단계에서 검사할 채널을 확인합니다.**Wireless > 802.11a Network**를 선택한 다음 그림과 같이 오른쪽의 Auto RF(자동 RF)를 선택합니다

.



Auto **RF** 페이지에서 아래로 스크롤하여 Noise/**Interference/Rogue Monitoring Channels**를 선택합니다

.



Channel List(채널 목록)에서는 다른 컨트롤러 및 AP 기능 외에 비인가 모니터링을 위해 스캔할 채널에 대해 자세히 설명합니다. 경량형 AP에 대한 자세한 내용은 경량 액세스 포인트 FAQ를 참조하고, 무선 LAN 컨트롤러(WLC) 문제 해결 FAQ에서 무선 컨트롤러에 대한 자세한 내용을 참조하십시오

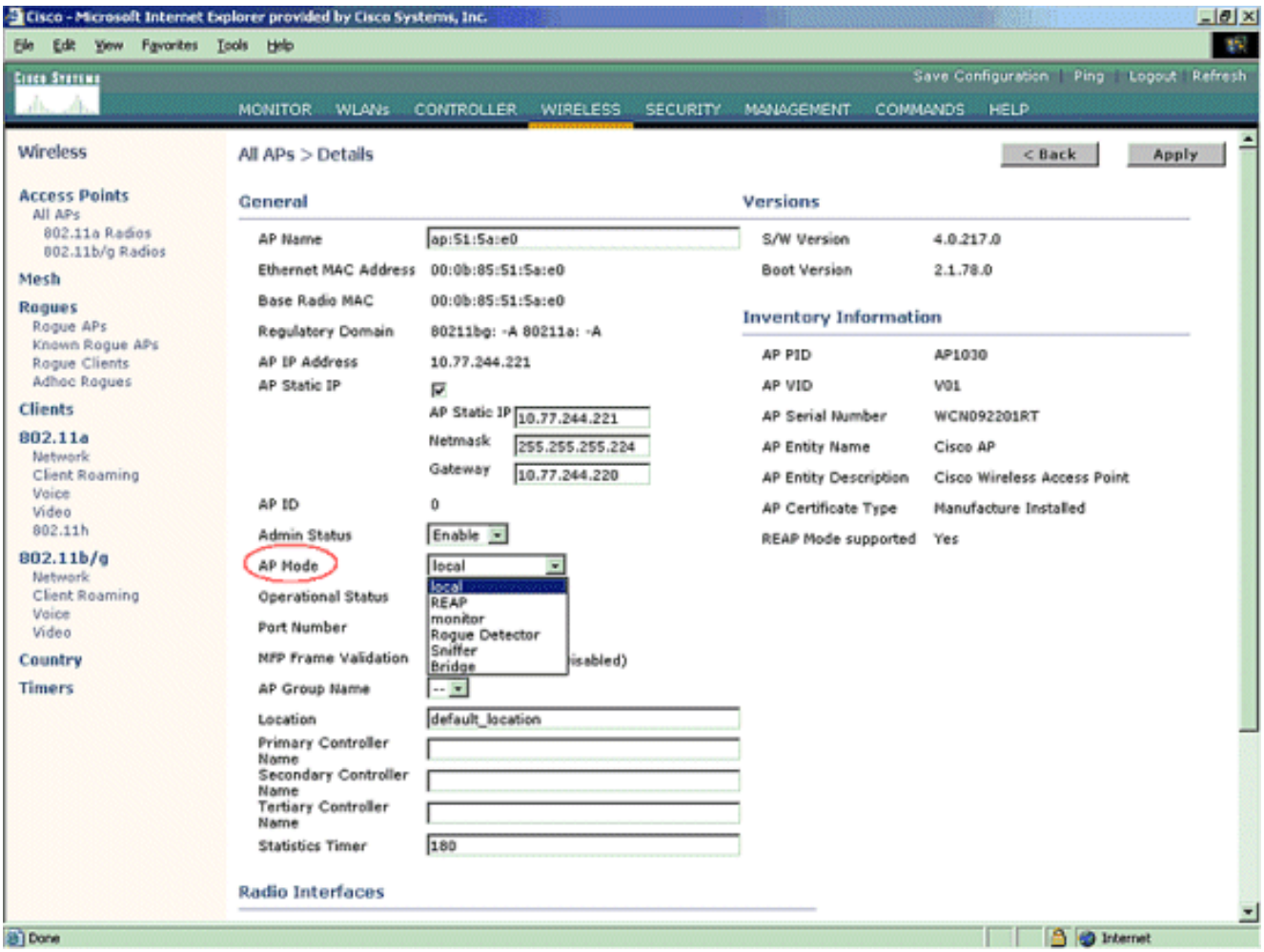
Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. 선택한 채널 스캔에 대한 기간 설정:정의된 채널 그룹의 검사 기간은 Monitor Intervals(**모니터 간격) > Noise Measurement(노이즈 측정)**에서 구성되며, 허용 범위는 60~3600초입니다. 기본값인 180초로 두면 AP는 채널 그룹의 각 채널을 180초마다 50ms씩 한 번씩 스캔합니다. 이 기간 동안 AP 라디오는 서비스 채널에서 지정된 채널로 변경되고 50ms의 값을 수신 대기하며 기록한 다음 원래 채널로 돌아갑니다. hop time과 50ms의 체류 시간은 매번 약 60ms 동안 AP 오프채널을 사용합니다. 즉, 각 AP는 총 180초 중 약 840ms의 비인가 수신 대기 시간을 소비합니다."listen" 또는 "체류" 시간은 수정할 수 없으며 노이즈 측정 값을 조정하여 변경되지 않습니다. 노이즈 측정 타이머가 낮아지면 비인가 검색 프로세스에서 더 많은 비인가를 찾아 더 빨리 찾을 수 있습니다. 그러나 이러한 개선은 데이터 무결성 및 클라이언트 서비스를 희생하

여 발생합니다. 반면, 더 높은 가치를 통해 데이터 무결성이 향상되지만 비인가를 신속하게 찾을 수 있는 능력이 줄어듭니다.

5. AP 작동 모드를 구성합니다.경량 AP 작동 모드는 AP의 역할을 정의합니다. 이 문서에 제시된 정보와 관련된 모드는 다음과 같습니다.**Local**(로컬) - AP의 정상적인 작업입니다. 이 모드를 사용하면 구성된 채널이 노이즈 및 비인가를 스캔하는 동안 데이터 클라이언트를 서비스할 수 있습니다. 이 작동 모드에서 AP는 50ms 동안 오프채널로 이동하여 비인가 수신 대기합니다. Auto RF 컨피그레이션에 지정된 기간 동안 각 채널을 한 번에 하나씩 순환합니다.**Monitor**(모니터) - 이 모드는 라디오 수신 전용 모드이며 AP가 구성된 모든 채널을 12초마다 스캔할 수 있도록 합니다. 이 방법으로 구성된 AP를 통해 인증 취소 패킷만 공기 중에 전송됩니다. 모니터 모드 AP는 비인가를 탐지할 수 있지만, RLDP 패킷을 전송하기 위해 의심스러운 비인가 패킷에 클라이언트로 연결할 수는 없습니다.**참고:** DCA는 기본 모드로 구성할 수 있는 비중첩 채널을 의미합니다.**Rogue Detector**—이 모드에서는 AP 라디오가 꺼지고 AP가 유선 트래픽만 수신합니다. 컨트롤러는 비인가 탐지기로 구성된 AP는 물론 의심되는 비인가 클라이언트 및 AP MAC 주소의 목록을 전달합니다. 비인가 탐지기는 ARP 패킷만 수신하며, 필요한 경우 트렁크 링크를 통해 모든 브로드캐스트 도메인에 연결할 수 있습니다.경량형 AP가 컨트롤러에 연결되면 개별 AP 모드를 간단하게 구성할 수 있습니다. AP 모드를 변경하려면 컨트롤러 웹 인터페이스에 연결하고 **무선**으로 이동합니다. 이 화면과 유사한 화면을 표시하려면 원하는 AP 옆의 Details(세부사항)를 클릭합니다

.



원하는 AP 작업 모드를 선택하려면 AP Mode 드롭다운 메뉴를 사용합니다.

문제 해결 명령

AP에서 컨피그레이션을 트러블슈팅하기 위해 다음 명령을 사용할 수도 있습니다.

- **show rogue ap summary**—이 명령은 경량형 AP에서 탐지된 비인가 AP 목록을 표시합니다.
- **show rogue ap detailed** ***<rogue ap의 MAC address>***—개별 비인가 AP에 대한 세부 정보를 보려면 이 명령을 사용합니다. 이 명령은 비인가 AP가 유선 네트워크에 연결되어 있는지 확인하는 데 도움이 됩니다.

결론

Cisco 중앙 집중식 컨트롤러 솔루션 내에서 비인가 탐지 및 억제는 업계에서 가장 효과적이고 가장 거슬리지 않는 방법입니다. 네트워크 관리자에게 제공되는 유연성을 통해 어떤 네트워크 요구 사항도 수용할 수 있는 맞춤화된 맞춤화가 가능합니다.

관련 정보

- RF 그룹 개요
- 기술 지원 및 문서 – Cisco Systems