Aironet 600 Series OfficeExtend 액세스 포인트 구성

목차

소개

이 문서에서는 Cisco Aironet® 600 Series OEAP(OfficeExtend Access Point)와 함께 사용할 Cisco WLAN(Wireless LAN) Controller를 구성하기 위한 요구 사항에 대한 정보를 제공합니다. Cisco Aironet 600 Series OEAP는 분할 모드 작업을 지원하며 WLAN 컨트롤러를 통한 컨피그레이션이 필요한 기능과 최종 사용자가 로컬로 구성할 수 있는 기능을 갖추고 있습니다. 이 문서에서는 적절한 연결 및 지원되는 기능 집합에 필요한 컨피그레이션에 대한 정보도 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Aironet 600 Series OEAP(OfficeExtend Access Point)를 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.

표기 규칙

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

배경 정보

설정 지침

- Cisco Aironet 600 Series OEAP는 Cisco 5508, WiSM-2 및 Cisco 2504에서 지원됩니다.
- Cisco Aironet 600 Series OEAP를 지원하는 첫 번째 컨트롤러 릴리스는 7.0.116.0입니다
- 컨트롤러의 관리 인터페이스는 라우팅 가능한 IP 네트워크에 있어야 합니다.
- UDP 포트 번호 5246 및 5247의 트래픽을 허용하려면 회사 방화벽 컨피그레이션을 변경해야 합니다.

Office Extend 솔루션 개요

- 사용자에게 회사 컨트롤러의 IP 주소가 지정된 액세스 포인트(AP)가 제공되거나, 사용자가 컨피그레이션 화면(설정 HTML 페이지)에서 컨트롤러의 IP 주소를 입력할 수 있습니다.
- 사용자가 홈 라우터에 AP를 연결합니다.
- AP는 홈 라우터에서 IP 주소를 얻고, 프라이밍 컨트롤러에 조인하고, 보안 터널을 생성합니다 .
- 그런 다음 Cisco Aironet 600 Series OEAP는 기업 SSID를 광고합니다. 이 SSID는 WAN을 통해 동일한 보안 방법 및 서비스를 사용자의 집으로 확장합니다.
- 원격 LAN이 구성된 경우 AP의 유선 포트 하나가 컨트롤러로 다시 터널링됩니다.
- 그런 다음 사용자는 개인 용도로 로컬 SSID를 추가로 활성화할 수 있습니다.

방화벽 컨피그레이션 지침

방화벽의 일반 컨피그레이션은 방화벽을 통해 CAPWAP 제어 및 CAPWAP 관리 포트 번호를 허용하는 것입니다. Cisco Aironet 600 Series OEAP 컨트롤러는 DMZ 영역에 배치할 수 있습니다.

참고: WLAN 컨트롤러와 Cisco Aironet 600 Series OEAP 사이의 방화벽에서 UDP 5246 및 5247 포트를 열어야 합니다.

이 다이어그램은 DMZ의 Cisco Aironet 600 Series OEAP 컨트롤러를 보여줍니다.

다음은 방화벽 구성의 예입니다.

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address X.X.X.X 255.255.255.224

!--- X.X.X.X represents a public IP address

!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 172.16.1.2 255.255.255.0
!
access-list Outside extended permit udp any host X.X.X.Y eq 5246

!--- Public reachable IP of corporate controller

access-list Outside extended permit udp any host X.X.X.Y eq 5247

!--- Public reachable IP of corporate controller

access-list Outside extended permit icmp any any
!
global (outside) 1 interface
nat (dmz) 1 172.16.1.0 255.255.255.0
static (dmz,outside) X.X.X.Y 172.16.1.25 netmask 255.255.255.255
access-group Outside in interface outside
```

내부 AP-Manager IP 주소를 CAPWAPP Discovery Response 패킷의 일부로 OfficeExtend AP에 전송하려면 컨트롤러 관리자가 AP-Manager 인터페이스에서 NAT가 활성화되어 있고 올바른 NATed IP 주소가 AP로 전송되는지 확인해야 합니다.

참고: 기본적으로 NAT가 활성화된 경우 WLC는 AP 검색 중에만 NAT IP 주소로 응답합니다. NAT 게이트웨이 내부 및 외부에 AP가 있는 경우 NAT IP 주소 및 비 NAT(내부) 관리 IP 주소로 응답하도록 WLC를 설정하려면 다음 명령을 실행합니다.

<#root>

config network ap-discovery nat-ip-only disable

참고: 이는 WLC에 NAT IP 주소가 있는 경우에만 필요합니다.

이 다이어그램은 WLC에 NAT IP 주소가 있는 경우 NAT가 활성화되었음을 보여줍니다.

참고: 이 컨피그레이션은 인터넷 라우팅 가능 IP 주소로 구성되며 방화벽 뒤에 구성되지 않은 컨트롤러에서는 필요하지 않습니다.

Office Extend AP-600 구성 단계

Cisco Aironet 600 Series OEAP는 WLC에 로컬 모드 액세스 포인트로 연결됩니다.

참고: Monitor, H-REAP, Sniffer, Rogue Detection, Bridge 및 SE-Connect 모드는 600 Series에서 지원되지 않으며 구성할 수 없습니다.

참고: 1040, 1130, 1140 및 3502i Series Access Point의 Cisco Aironet 600 Series OEAP 기능을 사용하려면 H-REAP(Hybrid REAP)를 위한 AP를 구성하고 AP의 하위 모드를 Cisco Aironet 600 Series OEAP로 설정해야 합니다. 600 Series는 로컬 모드를 사용하므로 변경할 수 없으므로 이 작업은 수행되지 않습니다.

MAC 필터링은 초기 조인 프로세스 중에 AP 인증에 사용되어 권한이 없는 Cisco Aironet 600 Series OEAP 장치가 컨트롤러에 조인하지 못하도록 할 수 있습니다. 이 이미지는 MAC 필터링을 활성화하고 AP 보안 정책을 구성하는 위치를 보여줍니다.

Ethernet MAC(Radio MAC 주소가 아님)가 여기에 입력됩니다. 또한 MAC 주소를 Radius 서버에 입력하는 경우 소문자를 사용해야 합니다. 이더넷 MAC 주소를 검색하는 방법에 대한 자세한 내용은 AP 이벤트 로그를 검토할 수 있습니다(자세한 내용은 나중에 설명).

WLAN 및 원격 LAN 구성 설정

Cisco Aironet 600 Series OEAP에는 물리적 원격 LAN 포트(노란색 포트 #4) 하나가 있습니다. 이는 WLAN의 구성 방식과 매우 유사합니다. 그러나 무선이 아니고 AP 뒷면의 유선 LAN 포트이기 때문에 원격 LAN 포트로 호출하여 관리합니다.

디바이스에는 물리적 포트가 하나뿐이지만, 허브나 스위치를 사용할 경우 최대 4개의 유선 클라이언트를 연결할 수 있습니다.

참고: 원격 LAN 클라이언트 제한은 스위치 또는 허브를 여러 디바이스의 원격 LAN 포트에 연결하거나 해당 포트에 연결된 Cisco IP Phone에 직접 연결하는 것을 지원합니다.

참고: 처음 4개의 디바이스만 디바이스 중 하나가 1분 이상 유휴 상태가 될 때까지 연결할 수 있습니다. 802.1x 인증을 사용하는 경우 유선 포트에서 둘 이상의 클라이언트를 사용하려고 시도하는 동안 문제가 발생할 수 있습니다.

참고: 이 수치는 컨트롤러 WLAN에 대해 지정된 15개 한도에 영향을 미치지 않습니다.

원격 LAN은 컨트롤러에 구성된 WLAN 및 게스트 LAN과 유사하게 구성됩니다.

WLAN은 무선 보안 프로필입니다. 회사 네트워크에서 사용하는 프로필입니다. Cisco Aironet 600 Series OEAP는 최대 2개의 WLAN과 1개의 원격 LAN을 지원합니다.

원격 LAN은 WLAN과 유사하지만, 이 이미지에 표시된 것처럼 액세스 포인트 뒤쪽의 유선 포트(포트 #4은 노란색)에 매핑됩니다.

참고: WLAN이 두 개 이상이거나 원격 LAN이 두 개 이상인 경우 모두 AP 그룹에 배치해야 합니다.

이 그림에서는 WLAN 및 원격 LAN이 구성된 위치를 보여줍니다.

이 그림에서는 샘플 OEAP 그룹 이름을 보여줍니다.

이 그림에서는 WLAN SSID 및 RLAN 컨피그레이션을 보여줍니다.

Cisco Aironet 600 Series OEAP를 AP 그룹에 입력하면 AP 그룹 컨피그레이션에 대해 동일한 제한인 2개의 WLAN 및 1개의 원격 LAN이 적용됩니다. 또한 Cisco Aironet 600 Series OEAP가 기본 그룹에 있는 경우(즉, 정의된 AP 그룹에 없는 경우) 이 제품은 상위 ID 집합을 지원하지 않으므로 WLAN/원격 LAN ID를 ID 8 미만으로 설정해야 합니다.

이 이미지에 표시된 대로 ID 세트를 8 미만으로 유지합니다.

참고: Cisco Aironet 600 Series OEAP에서 사용 중인 WLAN 또는 원격 LAN을 변경할 목적으로 추가 WLAN 또는 원격 LAN을 생성하는 경우, 600 Series에서 새 WLAN 또는 원격 LAN을 활성화하기 전에 제거할 현재 WLAN 또는 원격 LAN을 비활성화합니다. AP 그룹에 대해 활성화된 원격 LAN이 두 개 이상인 경우 모든 원격 LAN을 비활성화한 다음 하나만 활성화합니다.

AP 그룹에 대해 활성화된 WLAN이 2개 이상인 경우 모든 WLAN을 비활성화한 다음 2개만 활성화합니다.

WLAN 보안 설정

WLAN에서 보안 설정을 설정할 때 600 Series에서 지원되지 않는 특정 요소가 있습니다.

레이어 2 보안의 경우 Cisco Aironet 600 Series OEAP에는 다음 옵션만 지원됩니다.

- 없음
- WPA+WPA2
- 고정 WEP는 사용할 수 있지만 .11n 데이터 전송률에는 사용할 수 없습니다.

참고: 802.1x 또는 PSK만 선택해야 합니다.

이 이미지에 표시된 대로 WPA의 보안 암호화 설정과 TKIP 및 AES의 WPA2의 보안 암호화 설정이 동일해야 합니다.

다음 이미지는 TKIP 및 AES에 대해 호환되지 않는 설정의 예를 제공합니다.

참고: 보안 설정에서는 지원되지 않는 기능을 허용합니다.

다음 이미지는 호환 가능한 설정의 예를 제공합니다.

MAC 필터링

보안 설정을 열어 두거나, MAC 필터링에 대해 설정하거나, 웹 인증에 대해 설정할 수 있습니다. 기본값은 MAC 필터링을 활용하는 것입니다.

이 그림에서는 레이어 2 및 레이어 3 MAC 필터링을 보여 줍니다.

QoS 설정은 다음과 같이 관리됩니다.

고급 설정도 관리해야 합니다.

참고:

- Coverage Hole Detection(커버리지 홀 탐지)을 활성화해서는 안 됩니다.
- Aironet IE(정보 요소)는 사용되지 않으므로 활성화해서는 안 됩니다.
- MFP(Management Frame Protection)도 지원되지 않으므로 이 이미지에 표시된 대로 비활성화하거나 선택 사항으로 구성해야 합니다.
- 클라이언트 로드 밸런싱 및 클라이언트 대역 선택은 지원되지 않으며 활성화해서는 안 됩니다.

지원되는 사용자 수

600 시리즈에 제공된 WLAN 컨트롤러 WLAN에는 한 번에 15명의 사용자만 연결할 수 있습니다. 16번째 사용자는 첫 번째 클라이언트 중 하나가 인증을 취소하거나 컨트롤러에서 시간 초과가 발생할 때까지 인증할 수 없습니다.

참고: 이 수치는 600 Series의 컨트롤러 WLAN 전체에 누적됩니다.

예를 들어 2개의 컨트롤러 WLAN이 구성되어 있고 WLAN 중 하나에 15명의 사용자가 있는 경우 600 시리즈에서 다른 WLAN에 가입할 수 있는 사용자는 없습니다. 이 제한은 최종 사용자가 개인 용도로 설계된 600 시리즈에서 구성하는 로컬 사설 WLAN에 적용되지 않으며, 이러한 사설 WLAN 또는 유선 포트에 연결된 클라이언트는 이러한 제한에 영향을 미치지 않습니다.

채널 관리 및 설정

600 시리즈의 무선 장치는 Wireless LAN Controller가 아닌 600 시리즈의 로컬 GUI를 통해 제어됩니다.

컨트롤러를 통해 스펙트럼 채널 제어, 전원 공급 또는 무선 비활성화 시도는 600 Series에 영향을 미치지 않습니다.

600 Series는 시작 중에 2.4GHz 및 5.0GHz에 대한 채널을 스캔하고 선택합니다. 단, 로컬 GUI의 기본 설정은 두 스펙트럼에서 모두 기본값으로 유지됩니다.

참고: 앞서 설명한 대로 사용자가 로컬에서 하나 또는 두 무선 모두 비활성화하면(해당 무선 장치는 기업 액세스에도 비활성화됨) RRM 및 모니터, H-REAP, 스니퍼 등의 고급 기능은 재택 근무자와 재택 근무자의 사용을 위해 배치된 Cisco Aironet 600 Series OEAP의 기능을 벗어납니다.

5.0GHz에 대한 채널 선택 및 대역폭은 Cisco Aironet 600 Series OEAP의 로컬 GUI에서 구성합니

다.

참고:

- 5GHz에서는 20 및 40MHz 와이드 설정을 사용할 수 있습니다.
- 2.4GHz 폭 40MHz는 지원되지 않으며 20MHz에서 고정됩니다.
- 40MHz 폭(채널 본딩)은 2.4GHz에서 지원되지 않습니다.

추가 주의 사항

Cisco Aironet 600 Series OEAP는 단일 AP 구축을 위해 설계되었습니다. 따라서 600 Series 간의 클라이언트 로밍은 지원되지 않습니다.

참고: 컨트롤러에서 802.11a/n 또는 802.11b/g/n을 비활성화하더라도 Cisco Aironet 600 Series OEAP에서 이러한 스펙트럼이 비활성화되지 않을 수 있습니다. 로컬 SSID가 여전히 작동 중일 수 있기 때문입니다.

최종 사용자는 Cisco Aironet 600 Series OEAP 내의 무선 장치에 대한 제어를 활성화/비활성화할 수 있습니다.

유선 포트에서 802.1x 지원

이 초기 릴리스에서는 802.1x가 CLI(Command Line Interface)에서만 지원됩니다.

참고: GUI 지원이 아직 추가되지 않았습니다.

Cisco Aironet 600 Series OEAP 뒷면의 유선 포트(노란색 포트 #4)이며 원격 LAN에 연결됩니다(원격 LAN 구성에 대한 이전 섹션 참조).

언제든지 show 명령을 사용하여 현재 원격 LAN 컨피그레이션을 표시할 수 있습니다.

```
<#root>

show remote-lan <remote-lan-id>
```

원격 LAN 컨피그레이션을 변경하려면 먼저 다음과 같이 비활성화해야 합니다.

```
<#root>

 remote-lan disable <remote-lan-id>
```

원격 LAN에 대해 802.1X 인증을 활성화합니다.

```
<#root>
```

config remote-lan security 802.1X enable <*remote-lan-id*>

다음 명령을 사용하여 실행 취소할 수 있습니다.

<#root>

config remote-lan security 802.1X disable <*remote-lan-id*>

원격 LAN의 경우 "Encryption(암호화)"은 항상 "None(없음)"(show remote-lan에 표시됨)이며 구성할 수 없습니다.

(컨트롤러에서) 로컬 EAP를 인증 서버로 사용하려면

<#root>

config remote-lan local-auth enable <*profile-name*> <*remote-lan-id*>

여기서 프로파일은 컨트롤러 GUI(Security > Local EAP) 또는 CLI(config local-auth)를 통해 정의됩니다. 이 명령에 대한 자세한 내용은 컨트롤러 가이드를 참조하십시오.

다음 명령을 사용하여 실행 취소할 수 있습니다.

<#root>

config remote-lan local-auth disable <*remote-lan-id*>

또는 외부 AAA 인증 서버를 사용하는 경우

- config remote-lan radius_server auth 추가/삭제 <remote-lan-id> <server-id>
- config remote-lan radius_server auth enable/disable <remote-lan-id>

여기서 서버는 컨트롤러 GUI(Security(보안) > RADIUS > Authentication(인증)) 또는 CLI(config radius auth)를 통해 구성됩니다. 이 명령에 대한 자세한 내용은 컨트롤러 설명서를 참조하십시오.

컨피그레이션을 완료한 후 원격 LAN을 활성화합니다.

<#root>

config remote-lan enable <*remote-lan-id*>

설정을 확인하려면 show remote-lan <remote-lan-id> 명령을 사용합니다.

원격 LAN 클라이언트의 경우 802.1X 인증을 활성화하고 그에 맞게 구성해야 합니다. 디바이스 사용 설명서를 참조하십시오.

OEAP-600 액세스 포인트 컨피그레이션

이 그림에서는 Cisco Aironet 600 Series OEAP의 배선 다이어그램을 보여줍니다.

Cisco Aironet 600 Series OEAP의 기본 DHCP 범위는 10.0.0.x이므로 주소 10.0.0.1을 사용하여 포트 1-3의 AP로 이동할 수 있습니다. 기본 사용자 이름과 비밀번호는 admin입니다.

참고: 이는 Cisco를 사용자 이름 및 비밀번호로 사용한 AP1040, 1130, 1140 및 3502i와 다릅니다.

무선 장치가 작동 중이고 개인 SSID가 이미 구성된 경우 구성 화면에 무선으로 액세스할 수 있습니다. 그렇지 않으면 로컬 이더넷 포트 1-3을 사용해야 합니다.

로그인하려면 기본 사용자 이름 및 비밀번호는 admin입니다.

참고: 노란색 포트 #4는 로컬에서 사용할 수 없습니다. 컨트롤러에 원격 LAN이 구성된 경우 AP가 컨트롤러에 성공적으로 연결되면 이 포트는 다시 터널링합니다. 디바이스를 찾아보려면 로컬에서 포트 1-3을 사용합니다.

디바이스를 성공적으로 탐색하면 홈 상태 화면이 표시됩니다. 이 화면에서는 무선 및 MAC 통계를 제공합니다. 무선 장치가 구성되지 않은 경우, 컨피그레이션 화면에서 사용자는 무선 장치를 활성화하고, 채널 및 모드를 설정하고, 로컬 SSID를 구성하고, WLAN 설정을 활성화할 수 있습니다.

SSID 화면에서 사용자가 개인 WLAN 네트워크를 구성할 수 있습니다. (컨트롤러의 IP로 WAN을 구성한 후) 회사 무선 SSID 및 보안 매개변수가 설정되고 컨트롤러에서 푸시다운되며, 성공적으로 조인했습니다.

이 그림에서는 SSID 로컬 MAC 필터링 컨피그레이션을 보여줍니다.

사용자가 개인 SSID를 구성하면 아래 화면에서 사용자가 개인 홈 SSID에 보안을 설정하고 무선 장치를 활성화하며 원하는 경우 MAC 필터링을 구성할 수 있습니다. 개인 네트워크에서 802.11n 속도를 사용하는 경우 사용자가 WPA2-PSK 및 AES를 활성화하는 인증 유형, 암호화 유형 및 암호를 선택하는 것이 좋습니다.

참고: 이러한 SSID 설정은 사용자가 하나 또는 둘 모두의 라디오를 비활성화하도록 선택하는 경우 기업 설정과 다릅니다(둘 다 기업 용도로 비활성화됨).

관리자 제어 설정에 로컬로 액세스할 수 있는 사용자는 관리자가 장치를 암호로 보호하고 구성하지 않는 한 라디오 활성화/비활성화와 같은 핵심 기능을 제어할 수 있습니다. 따라서 두 무선 장치를 모두 비활성화하지 않도록 주의해야 합니다. 이렇게 하면 디바이스가 성공적으로 컨트롤러에 조인하더라도 연결이 손실될 수 있습니다.

이 그림에서는 시스템 보안 설정을 보여 줍니다.

이 제품은 홈 라우터의 기능을 대체하도록 설계되지 않았으므로 홈 재택근무자는 홈 라우터 뒤에

Cisco Aironet 600 Series OEAP를 설치할 것으로 예상됩니다. 이 제품의 현재 버전에는 방화벽 지원, PPPoE 지원 또는 포트 전달이 없기 때문입니다. 이러한 기능은 고객이 홈 라우터에서 찾을 수 있기를 기대하는 기능입니다.

이 제품은 홈 라우터 없이 작동할 수 있지만 명시된 이유로 인해 이 제품을 그렇게 배치하지 않는 것이 좋습니다. 또한 일부 모뎀에 직접 연결하는 데 호환성 문제가 있을 수 있습니다.

대부분의 홈 라우터에 192.168.x.x 범위의 DHCP 범위가 있는 경우 이 디바이스는 기본 DHCP 범위가 10.0.0.x이며 구성 가능합니다.

홈 라우터가 10.0.0.x를 사용하는 경우 네트워크 충돌을 방지하기 위해 192.168.1.x 또는 호환 가능한 IP 주소를 사용하도록 Cisco Aironet 600 Series OEAP를 구성해야 합니다.

이 그림에서는 DHCP 범위 컨피그레이션을 보여줍니다.

주의: IT 관리자가 Cisco Aironet 600 Series OEAP를 준비하거나 구성하지 않은 경우 사용자가 회사 컨트롤러의 IP 주소를 입력해야 AP가 컨트롤러에 성공적으로 조인할 수 있습니다(아래 참조). 가입이 성공적으로 완료되면 AP는 컨트롤러에서 최신 이미지와 회사 WLAN 설정과 같은 컨피그레이션 매개변수를 다운로드해야 합니다. 또한 구성된 경우 원격 LAN 설정 유선 포트는 Cisco Aironet 600 Series OEAP 뒷면에 #4.

연결되지 않을 경우 컨트롤러의 IP 주소가 인터넷을 통해 연결할 수 있는지 확인합니다. MAC 필터링이 활성화된 경우 MAC 주소가 컨트롤러에 성공적으로 입력되었는지 확인합니다.

이 그림에서는 Cisco Aironet 600 Series OEAP 컨트롤러의 IP 주소를 보여줍니다.

OEAP-600 액세스 포인트 하드웨어 설치

이 그림에서는 Cisco Aironet 600 Series OEAP의 물리적 측면을 보여줍니다.

이 AP는 테이블에 장착할 수 있도록 설계되었으며 고무 받침을 가지고 있습니다. 벽 장착이 가능하거나, 제공된 거치대를 사용하여 똑바로 앉을 수도 있습니다. AP를 원하는 사용자와 최대한 가깝게 찾으십시오. 금속 책상 위 또는 큰 거울 근처에 장치를 두는 것과 같이 금속 표면이 큰 영역은 피하십시오. AP와 사용자 사이에 더 많은 장벽과 객체가 있으므로 신호 강도가 저하되고 성능이 저하될 수 있습니다.

참고: 이 AP는 +12V 전원 공급 장치를 사용하며 PoE(Power over Ethernet)를 사용하지 않습니다. 또한 디바이스는 PoE를 제공하지 않습니다. 올바른 전원 어댑터를 AP와 함께 사용해야 합니다. 또한 랩톱, IP 전화 등 다른 장치의 다른 어댑터를 사용하면 AP가 손상될 수 있으므로 사용하지 마십시오.

장치는 플라스틱 앵커 또는 나무 나사로 벽에 장착 할 수 있습니다.

상기 유닛은, 상기 공급된 거치대를 사용하여, 직립으로 거치될 수 있다.

Cisco Aironet 600 Series OEAP에는 AP 가장자리에 안테나가 있습니다. 사용자는 신호가 방향성이나 감소되는 금속 물체 또는 장애물 근처의 영역에 AP를 배치하지 않도록 주의해야 합니다. 안테나 이득은 두 대역에서 약 2dBi이며 360도 패턴으로 방사되도록 설계되었습니다. 전구(램프 음영 없음)와 비슷하게 모든 방향으로 방사하는 것이 목표입니다. AP를 램프와 같이 생각하고 사용자에

게 가까이 두려고 합니다.

거울과 같은 금속 물체는 전등갓의 비유처럼 신호를 방해한다. 신호가 고체 물체를 관통하거나 통과해야 하는 경우 처리량 또는 범위가 저하될 수 있습니다. 3층 가정과 같이 연결이 필요한 경우 AP를 지하실 위치에 두지 말고 AP를 가정 내의 중앙 위치에 장착해 보십시오.

액세스 포인트에는 6개의 안테나(대역당 3개)가 있습니다.

이 그림에서는 2.4GHz 안테나 방사 패턴(왼쪽 하단 안테나에서 가져옴)을 보여 줍니다.

이 그림에서는 5GHz 안테나 방사 패턴(오른쪽 중간 안테나에서 가져옴)을 보여 줍니다.

OEAP-600 문제 해결

초기 배선이 올바른지 확인합니다. 그러면 Cisco Aironet 600 Series OEAP의 WAN 포트가 라우터에 연결되어 있고 IP 주소를 성공적으로 수신할 수 있음을 확인합니다. AP가 컨트롤러에 조인하는 것처럼 보이지 않으면 PC를 포트 1-3(홈 클라이언트 포트)에 연결하고 기본 IP 주소 10.0.0.1을 사용하여 AP를 탐색할 수 있는지 확인합니다. 기본 사용자 이름 및 비밀번호는 admin입니다.

기업 컨트롤러의 IP 주소가 설정되어 있는지 확인합니다. 그렇지 않은 경우 IP 주소를 입력하고 Cisco Aironet 600 Series OEAP를 리부팅하여 컨트롤러에 대한 링크를 설정하려고 시도합니다.

참고: 기업 포트 #4(노란색)는 컨피그레이션을 위해 디바이스를 탐색하는 데 사용할 수 없습니다. 이는 원격 LAN이 구성되지 않는 한 기본적으로 "데드 포트"입니다. 그런 다음 기업(유선 엔터프라이즈 연결에 사용됨)으로 다시 터널링합니다.

이벤트 로그를 확인하여 연결이 어떻게 진행되었는지 확인합니다(나중에 자세히 설명).

이 그림에서는 Cisco Aironet 600 Series OEAP 와이어링 다이어그램을 보여줍니다.

이 그림에서는 Cisco Aironet 600 Series OEAP 연결 포트를 보여줍니다.

Cisco Aironet 600 Series OEAP가 컨트롤러에 조인하지 못할 경우 다음 항목을 확인하는 것이 좋습니다.

1. 라우터가 작동하며 Cisco Aironet 600 Series OEAP의 WAN 포트에 연결되어 있는지 확인합니다.
2. Cisco Aironet 600 Series OEAP의 포트 1-3 중 하나에 PC를 연결합니다. 인터넷을 볼 수 있어야 합니다.
3. 회사 컨트롤러의 IP 주소가 AP에 있는지 확인합니다.
4. 컨트롤러가 DMZ에 있고 인터넷을 통해 연결할 수 있는지 확인합니다.
5. 참가를 확인하고 Cisco 로고 LED가 파란색 또는 보라색인지 확인합니다.
6. AP가 새 이미지를 로드하고 다시 시작해야 하는 경우 충분한 시간을 허용합니다.
7. 방화벽을 사용 중인 경우 UDP 5246 및 5247 포트가 차단되지 않았는지 확인합니다.

이 그림에서는 Cisco Aironet 600 Series OEAP 로고 LED 상태를 보여줍니다.

조인 프로세스가 실패하면 LED가 색상을 순환하거나 주황색으로 깜박입니다. 이 경우 이벤트 로그에서 자세한 내용을 확인하십시오. 이벤트 로그를 보려면 AP(개인 SSID 또는 유선 포트 1-3 사용)로 이동하여 IT 관리자가 검토할 수 있도록 이 데이터를 캡처합니다.

이 그림에서는 Cisco Aironet 600 Series OEAP 이벤트 로그를 보여 줍니다.

조인 프로세스가 실패하고 Cisco Aironet 600 Series OEAP가 컨트롤러에 처음으로 연결을 시도한 경우 Cisco Aironet 600 Series OEAP에 대한 AP 조인 통계를 확인합니다. 이렇게 하려면 AP의 Base Radio MAC이 필요합니다. 이벤트 로그에서 찾을 수 있습니다. 다음은 이를 해석하는 데 도움이 되는 설명이 포함된 이벤트 로그의 예입니다.

이를 알게 되면 컨트롤러 모니터 통계를 통해 Cisco Aironet 600 Series OEAP가 컨트롤러에 가입했는지 또는 컨트롤러에 가입했는지를 확인할 수 있습니다. 또한, 이는 장애가 발생한 이유 또는 장애가 발생한 경우에 대한 표시를 제공해야 합니다.

AP 인증이 필요한 경우 Cisco Aironet 600 Series OEAP Ethernet MAC 주소(라디오 MAC 주소가 아님)가 Radius 서버에 입력되었는지 확인합니다. 이벤트 로그에서 이더넷 MAC 주소도 확인할 수 있습니다.

컨트롤러에서 Cisco Aironet 600 Series OEAP 검색

로컬 이더넷 포트에 연결된 PC에서 인터넷에 액세스할 수 있지만 AP가 여전히 컨트롤러에 조인할 수 없는 경우, 컨트롤러 IP 주소가 로컬 AP GUI에 구성되어 있고 도달 가능한 상태임을 확인한 다음 AP가 성공적으로 조인되었는지 확인합니다. AP가 AAA 서버에 없는 것 같습니다. 또는 DTLS 핸드셰이킹이 실패할 경우 AP에 잘못된 인증서 또는 컨트롤러의 날짜/시간 오류가 있을 수 있습니다.

컨트롤러에 연결할 수 있는 Cisco Aironet 600 Series OEAP 장치가 없는 경우 컨트롤러가 DMZ에 있고 UDP 포트 5246 및 5247이 열려 있는지 확인합니다.

클라이언트 연결 문제를 디버그하는 방법

AP가 컨트롤러에 올바르게 연결되지만 무선 클라이언트가 기업 SSID와 연결할 수 없습니다. 이벤트 로그를 확인하여 연결 메시지가 AP에 도달하는지 확인합니다.

다음 그림은 WPA 또는 WPA2를 사용하는 기업 SSID와의 클라이언트 연결에 대한 일반적인 이벤트를 보여줍니다. 개방 인증 또는 고정 WEP를 사용하는 SSID의 경우 ADD MOBILE 이벤트가 하나만 있습니다.

이벤트 로그 - 클라이언트 연결

(Re)Assoc-Req 이벤트가 로그에 없는 경우 클라이언트에 올바른 보안 설정이 있는지 확인합니다.

(Re)Assoc-Req 이벤트가 로그에 표시되지만 클라이언트가 제대로 연결할 수 없는 경우, 클라이언트에 대해 컨트롤러에서 debug client <MAC address> 명령을 활성화하고 다른 Cisco 비 OEAP 액세스 포인트와 함께 작업하는 클라이언트와 동일한 방법으로 문제를 조사합니다.

이벤트 로그를 해석하는 방법

코멘트가 포함된 다음 이벤트 로그는 다른 Cisco Aironet 600 Series OEAP 연결 문제를 해결하는 데 도움이 될 수 있습니다.

다음은 Cisco Aironet 600 Series OEAP 이벤트 로그 파일에서 수집된 몇 가지 샘플과 이벤트 로그 해석에 도움이 되는 설명입니다.

인터넷 연결이 불안정할 때

이 섹션의 이벤트 로그 예는 인터넷 연결이 실패하거나 매우 느리거나 간헐적으로 끝날 때 발생할 수 있습니다. ISP 네트워크, ISP 모뎀 또는 홈 라우터에 의해 발생할 수 있습니다. ISP의 연결이 끊기거나 불안정해지는 경우가 있습니다. 이 경우 CAPWAP 링크(다시 회사로 터널)에 오류가 발생하거나 문제가 발생할 수 있습니다.

다음은 이벤트 로그에서 이러한 실패의 예입니다.

추가 debug 명령

호텔 또는 기타 유료 사용 장소에서 Cisco Aironet 600 Series OEAP를 사용할 경우, Cisco Aironet 600 Series OEAP가 컨트롤러로 다시 터널링하기 전에 벽으로 둘러싸인 정원을 통과해야 합니다. 이를 위해서는 유선 로컬 포트(포트 1-3) 중 하나에 노트북을 꽂거나 개인 SSID를 사용하여 호텔에 로그인하고 스플래시 화면을 만족해야 합니다.

AP의 홈측에서 인터넷 연결이 이루어지면 유닛에서는 DTLS 터널과 회사 SSID를 설정합니다. 그러면 유선 포트 #4(원격 LAN이 구성된 것으로 가정)이 활성화됩니다.

참고: 이 작업에는 몇 분 정도 걸릴 수 있습니다. Cisco 로고 LED에서 파란색 또는 보라색이 단색으로 표시되는지 확인하여 성공적인 참여를 알려 주십시오. 이 시점에서는 개인 연결과 기업 연결이 모두 활성화되어 있습니다.

참고: 호텔 또는 다른 ISP의 연결이 끊기면 터널이 중단됩니다(일반적으로 24시간). 그런 다음 동일한 프로세스를 다시 시작해야 합니다. 이것은 설계에 의한 것이며 정상입니다.

이 그림에서는 Office Extend를 Pay-for-Use 구성으로 보여 줍니다.

이 그림에서는 추가 debug 명령(무선 인터페이스 정보)을 보여 줍니다.

알려진 문제/주의 사항

컨피그레이션 파일을 컨트롤러에서 TFTP/FTP 서버로 업로드하면 원격 LAN 컨피그레이션이 WLAN 컨피그레이션으로 업로드됩니다. 자세한 내용은 Cisco Wireless LAN Controller 릴리스 정보 및 Lightweight Access Points for Release 7.0.116.0을 참조하십시오.

OEAP-600에서 컨트롤러의 인증 실패로 인해 CAPWAP 연결이 실패하는 경우 OEAP-600에서 CISCO 로고 LED가 잠시 동안 꺼진 후 OEAP-600이 CAPWAP 시도를 재시작할 수 있습니다. 이는 정상이므로 로고 LED가 잠시 꺼질 때 AP가 종료되지 않았음을 알고 있어야 합니다.

이 OEAP-600 제품은 이전 OEAP 액세스 포인트와 다른 로그인 이름을 가지고 있습니다. Linksys와 같은 홈 제품과 일관되게 하려면 기본 사용자 이름은 admin의 비밀번호로 admin입니다. 다른 Cisco

OEAP 액세스 포인트(예: AP-1130 및 AP-1140)는 Cisco의 비밀번호로 Cisco의 기본 사용자 이름을 가집니다.

OEAP-600의 첫 번째 릴리스는 802.1x를 지원하지만 CLI에서만 지원됩니다. GUI를 변경하려고 시도하는 사용자는 컨피그레이션을 잃을 수 있습니다.

호텔 또는 기타 유료 사용 장소에서 OEAP-600을 사용할 경우, OEAP-600이 컨트롤러로 다시 터널링하기 전에 벽 정원을 통과해야 합니다. 노트북 컴퓨터를 유선 로컬 포트(포트 1-3) 중 하나에 연결하거나 개인 SSID 로그로 호텔에 로그인하면 스플래시 화면이 나타납니다. AP의 홈측에서 인터넷 연결이 이루어지면 유닛에서는 DTLS 터널, 회사 SSID 및 유선 포트 #4을 설정하며, 이 경우 Remote-LAN이 구성된 것으로 간주하고 활성화됩니다. 이 작업에는 몇 분 정도 걸릴 수 있습니다. Cisco 로고 LED에서 파란색 또는 보라색을 확인하면 정상적으로 참가했음을 알 수 있습니다. 이 시점에서는 개인 연결과 기업 연결이 모두 활성화되어 있습니다.

참고: 호텔 또는 기타 ISP의 연결이 끊기면(일반적으로 24시간) 터널이 끊어질 수 있으며 동일한 프로세스를 다시 시작해야 합니다. 이것은 설계에 의한 것이며 정상입니다.

Office Extend in pay for use 장소

다음은 Cisco 7.2 릴리스에서 추가된 몇 가지 개선 사항입니다.

- GUI에 802.1x 보안 추가
- 컨트롤러에서 AP의 로컬 WLAN 액세스를 비활성화하는 기능 - 개인 SSID를 비활성화하여 기업 컨피그레이션만 허용
- 채널 할당 선택 가능 옵션
- 2개의 기업 SSID에서 3개의 SSID로 지원 변경
- 듀얼 RLAN 포트 기능 지원

GUI에 802.1x 보안 추가

이제 802.1x가 GUI에 추가되었습니다.

원격 LAN 포트 인증에 대한 참고 사항.

컨트롤러에서 AP의 로컬 WLAN 액세스를 비활성화하는 기능 - 개인 SSID를 비활성화하여 기업 컨피그레이션만 허용

로컬 WLAN 액세스 비활성화

채널 할당 선택 가능 옵션은 다음과 같습니다.

- 로컬로 제어되는 AP
- WLC 제어됨

RF 채널 및 전력 할당이 로컬 또는 WLC로 제어됨

듀얼 RLAN 포트 기능 지원(CLI만 해당)

이 메모는 OEAP-600 이더넷 포트 3이 원격 LAN으로 작동할 수 있도록 하는 듀얼 RLAN 포트 기능을 사용하는 OEAP-600 시리즈 AP에 적용됩니다. 컨피그레이션은 CLI를 통해서만 허용되며, 그 예는 다음과 같습니다.

```
Config network oeap-600 dual-rlan-ports enable|disable
```

이 기능이 구성되지 않은 경우 단일 포트 4 원격 LAN이 계속 작동합니다. 각 포트는 각 포트에 대해 고유한 원격 LAN을 사용합니다. 원격 LAN 매핑은 기본 그룹을 사용하는지 AP 그룹을 사용하는지에 따라 달라집니다.

기본 그룹

default-group을 사용하는 경우 짝수 원격 LAN ID가 있는 단일 원격 LAN이 포트 4에 매핑됩니다. 예를 들어 remote-lan-id 2가 있는 remote-lan은 OEAP-600의 포트 4에 매핑됩니다. 홀수 번호의 원격 LAN ID가 있는 원격 LAN은 포트 3(OEAP-600)에 매핑됩니다.

예를 들어, 다음 두 개의 remote-lan을 예로 들 수 있습니다.

```
(Cisco Controller) >show remote-lan summary

Number of Remote LANS.............................. 2

RLAN ID  RLAN Profile Name    Status    Interface Name
-------  -----------------------------------  --------  --------------------
2        rlan2                                Enabled   management
3        rlan3                                Enabled   management
```

rlan2에는 짝수 원격 lan ID, 2가 있으므로 포트 4에 매핑됩니다. rlan3에는 홀수 원격 lan ID 3이 있으므로 포트 3에 매핑됩니다.

AP 그룹

AP 그룹을 사용하는 경우 OEAP-600 포트에 대한 매핑은 AP 그룹 순서에 따라 결정됩니다. AP 그룹을 사용하려면 먼저 AP 그룹에서 모든 원격 LAN 및 WLAN을 삭제하고 비워두어야 합니다. 그런 다음 AP 그룹에 2개의 remote-lan을 추가합니다. 먼저 포트 3 AP remote-LAN을 추가한 다음 포트 4 원격 그룹을 추가하고 마지막으로 WLAN을 추가합니다.

다음 예와 같이 목록의 첫 번째 위치에 있는 remote-lan은 포트 3에 매핑되고, 목록의 두 번째 위치는 포트 4에 매핑됩니다.

```
RLAN ID  RLAN Profile Name      Status    Interface Name
```

```
-------  ------------------------------------  --------  --------------------
2        rlan2                                 Enabled   management
3        rlan3                                 Enabled   management
```

관련 정보

- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 7.0
- 기술 지원 및 문서 – Cisco Systems

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.