실내 메시 구축 설명서

목차

소개

Lightweight Access Point 1242/1131은 선택한 실내 구축을 위한 2개의 무선 Wi-Fi 인프라 장치입니다.LWAPP(Lightweight Access Point Protocol) 기반 제품입니다.802.11b/g 및 802.11a와 호환되는 2.4GHz 라디오 및 5.8GHz 무선 장치를 제공합니다.액세스 포인트(AP)에 대한 로컬(클라이언트) 액세스에 하나의 라디오를 사용할 수 있으며 두 번째 라디오는 무선 백홀에 대해 구성할 수 있습니다.LAP1242/LAP1131은 P2P, P2MP 및 메시 유형의 아키텍처를 지원합니다.

설치를 시도하기 전에 반드시 가이드를 읽어 보십시오.

이 문서에서는 실내 메쉬용 Enterprise Wireless Mesh 구축에 대해 설명합니다.이 문서를 통해 무선 최종 사용자는 실내 메쉬의 기본 사항, 실내 메쉬를 구성할 위치 및 실내 메쉬를 구성하는 방법을 이해할 수 있습니다.실내 메쉬는 무선 컨트롤러 및 경량 AP를 사용하여 구축된 Cisco Enterprise Wireless Mesh의 하위 집합입니다.

실내 메쉬는 Unified Wireless 아키텍처에 구축된 엔터프라이즈 메시 아키텍처의 하위 집합입니다.현재 실내 메쉬가 수요가 많습니다.실내 메쉬에서는 무선 장치(일반적으로 802.11b/g) 중 하나 및/또는 유선 이더넷 링크를 사용하여 클라이언트에 연결하는 반면, 두 번째 라디오(일반적으로 802.11a)는 클라이언트 트래픽을 백홀하는 데 사용됩니다.백홀은 단일 홉이거나 다중 홉이 될 수 있습니다.실내 메쉬는 다음과 같은 값을 제공합니다.

- 각 AP에 이더넷 배선을 실행할 필요가 없습니다.
- 각 AP에는 이더넷 스위치 포트가 필요하지 않습니다.
- 와이어가 연결을 제공할 수 없는 네트워크 연결
- 구축 유연성 - 이더넷 스위치에서 100m로 제한되지 않음
- Ad-Hoc 무선 네트워크를 쉽게 구축할 수 있습니다.

앞서 언급한 이유뿐만 아니라 배선 비용 절감으로 인해 대형 박스 소매업체는 실내 메시에 매우 매력을 느끼고 있습니다.

재고 전문가들은 소매업체, 제조 공장 및 기타 회사에 대한 재고 실사를 수행하는 데 이 보고서를 사용합니다.이들은 고객 사이트에 임시 Wi-Fi 네트워크를 신속하게 구축하여 휴대용 장치에 실시간 연결을 구현하고자 합니다.교육 세미나, 회의, 제조 및 접대는 실내 메시 아키텍처가 필요한 장소 중 일부입니다.

이 가이드를 다 읽으면 사용 위치와 실내 메시 구성 방법을 이해할 수 있습니다.또한 NEMA 엔클로저의 실내 메쉬는 실외 메쉬를 대체하는 것이 아니라는 것을 알 수 있습니다.또한 자율 AP에서 사용하는 링크 역할 유연성(단일 홉의 메시)보다 실내 메쉬의 우수성을 이해할 수 있습니다.

가정:

Cisco Unified Wireless Network, 아키텍처 및 제품에 대한 지식을 보유하고 있습니다.Cisco Outdoor Mesh 제품과 메시 네트워킹에 사용되는 일부 용어에 대해 알고 있습니다.

약어 용어	
LWAPP	Lightweight Access Point Protocol - AP와 무선 LAN

	컨트롤러 간의 제어 및 데이터 터널링 프로토콜입니다.
WLAN 컨트롤러 /컨트롤러 /WLC	Wireless LAN Controller - 다수의 매니지드 엔드포인트를 단일 통합 시스템으로 축소하여 WLAN의 네트워크 관리를 중앙 집중화하고 간소화하는 Cisco 디바이스로, 통합 인텔리전트 정보 WLAN 네트워크 시스템을 지원합니다.
RAP	루트 액세스 포인트/루프 액세스 포인트 - Cisco 무선 장치는 컨트롤러와 다른 무선 AP 간의 브리지 역할을 합니다.컨트롤러에 연결된 AP입니다.
맵	메시 AP - 802.11a 무선 장치의 RAP 또는 MAP에 연결되고 802.11b/g 무선 장치의 클라이언트에도 서비스를 제공하는 Cisco 무선 장치입니다.
상위	802.11a 라디오에서 공중에서 다른 AP에 대한 액세스를 제공하는 AP(RAP/MAP).
네이버	메시 네트워크의 모든 AP는 네이버이며 네이버가 있습니다.RAP에 컨트롤러에 연결된 인접 디바이스가 없습니다.
자식	컨트롤러에서 더 멀리 떨어진 AP는 항상 하위 AP입니다.자식은 메시 네트워크에 부모 및 인접 디바이스가 하나씩 있습니다.상위 항목이 사망한 경우 가장 쉬운 값을 가진 다음 인접 디바이스가 상위 항목이 선택됩니다.
SNR	신호 대 잡음 비율
BGN	브리지 그룹 이름
EAP	확장 가능 한 인증 프로토콜
PSK	사전 공유 키
AWPP	적응형 무선 경로 프로토콜

개요

Cisco Indoor Mesh Network Access Point는 선택한 실내 구축을 위한 2개의 무선 Wi-Fi 인프라 장치입니다.LWAPP(Lightweight Access Point Protocol) 기반 제품입니다.802.11b/g, 802.11a 표준과

호환되는 2.4GHz 라디오 및 5.8GHz 무선 장치를 제공합니다.AP의 로컬(클라이언트) 액세스에 하나의 라디오(802.11b/g)를 사용할 수 있으며, 무선 백홀에 대해 두 번째 라디오(802.11a)를 구성할 수 있습니다.백홀을 통해 서로 다른 노드(무선)가 서로 통신하고 로컬 클라이언트 액세스도 제공하는 실내 메시 아키텍처를 제공합니다.이 AP는 point-to-point 및 point-to-multipoint 브리징 아키텍처에도 사용할 수 있습니다.무선 실내 메시 네트워크 솔루션은 최소 인프라에서 높은 데이터 전송률과 우수한 안정성을 확보할 수 있으므로 넓은 실내 적용 범위에 이상적입니다.다음은 이 제품의 첫 번째 릴리스와 함께 도입된 기본 핵심 기능입니다.

- 실내 환경에서 3개의 hop-count에 사용됩니다.최대 4개.
- 최종 사용자 클라이언트에 대한 노드 및 호스트를 릴레이합니다.802.11a 라디오는 클라이언트 서비스를 위해 백홀 인터페이스와 802.11b/g 라디오는 사용됩니다.
- 실내 메시 AP 보안 - EAP 및 PSK가 지원됩니다.
- 메시 환경의 LWAPP MAP은 이더넷 연결 AP와 동일한 방식으로 컨트롤러와 통신합니다.
- 포인트 투 포인트 무선 브리징
- 포인트-투-멀티포인트 무선 브리징.
- 최적의 상위 선택.SNR, EASE 및 BGN
- BGN 개선 사항NULL 및 기본 모드입니다.
- 로컬 액세스.
- 상위 블랙리스트.제외 목록입니다.
- AWPP를 통한 자가 복구
- 이더넷 브리징.
- 4.0 릴리스의 기본 Voice 지원
- 동적 주파수 선택.
- Anti-stranding - 기본 BGN 및 DHCP 장애 조치.

참고: 다음 기능은 지원되지 않습니다.

- 4.9GHz 공공 안전 채널
- 간섭 관련 라우팅
- 백그라운드 검사
- 범용 액세스
- 작업 그룹 브리지 지원

실내 메시 소프트웨어

실내 메시 소프트웨어는 실내 AP, 특히 실내 메쉬에 집중하기 때문에 특별 릴리스입니다.이 릴리스에서는 실내 AP가 모두 로컬 모드와 브리지 모드에서도 작동합니다.4.1.171.0 릴리스에서 사용할 수 있는 일부 기능은 이 릴리스에서 구현되지 않습니다.CLI(Command Line Interface), GUI(Graphical User Interface)(GUI - 웹 브라우저) 및 상태 시스템 자체도 향상되었습니다.이러한 개선 사항의 목표는 이 신제품과 그 기능의 실행 가능성에 대한 귀하의 관점에서 귀중한 정보를 얻는 것입니다.

실내 메시 관련 개선 사항:

- **실내 환경** - 실내 메쉬는 LAP1242s 및 LAP1131을 사용하여 구현됩니다. 이러한 메쉬는 이더넷 케이블을 사용할 수 없는 실내 환경에서 구현됩니다.구현은 건물 내 원격 지역(예: 소매 유통 센터, 세미나/컨퍼런스 교육, 제조, 숙박 등)에 무선 커버리지를 쉽고 빠르게 제공할 수 있습니다.
- **BGN(Bridge Group Name) 개선 사항** - 네트워크 관리자가 실내 메시 AP의 네트워크를 사용자 지정 섹터로 구성할 수 있도록 Cisco는 브리지 그룹 이름(BGN)이라는 메커니즘을 제공합니다.실제로 섹터 이름인 BGN은 AP가 동일한 BGN을 사용하여 다른 AP에 연결하도록 합니다.AP가 BGN과 일치하는 적합한 섹터를 찾지 못할 경우 AP는 기본 모드에서 작동하며 기본

BGN에 응답하는 최상의 부모를 선택합니다.이 기능은 고립된 AP 조건(누군가 BGN을 잘못 구성한 경우)에 맞서 싸우는 동안 이미 현장에서 많은 평가를 받았습니다. 4.1.171.0 소프트웨어 릴리스에서는 기본 BGN을 사용할 때 AP가 실내 메시 노드로 작동하지 않으며 클라이언트 액세스 권한이 없습니다.컨트롤러를 통해 액세스할 수 있는 유지 보수 모드이며, 관리자가 BGN을 수정하지 않으면 30분 후에 AP가 재부팅됩니다.

- **보안 개선** - 실내 메시 코드의 보안은 기본적으로 EAP(Extensible Authentication Protocol)에 대해 구성됩니다. 이는 RFC3748에 정의되어 있습니다. EAP 프로토콜은 무선 LAN에 한정되지 않고 유선 LAN 인증에 사용할 수 있지만 무선 LAN에서 가장 많이 사용됩니다.802.11 a/b/g 무선 액세스 포인트와 같은 802.1X 지원 NAS(Network Access Server) 장치에 의해 EAP가 호출되는 경우, 최신 EAP 방법은 안전한 인증 메커니즘을 제공하고 클라이언트와 NAS 간에 보안 PMK(Pair-wise Master Key)를 협상할 수 있습니다.그런 다음 PMK를 TKIP 또는 CCMP(AES 기반) 암호화를 사용하는 무선 암호화 세션에 사용할 수 있습니다.4.1.171.0 소프트웨어 릴리스 이전에는 실외 메시 AP에서 컨트롤러에 조인하는 데 PMK/BMK를 사용했습니다.이는 3주기 과정이었습니다.이제 통합 시간을 단축할 수 있습니다.실내 메시 보안의 전반적인 목표는 다음과 같습니다.보안 프로비저닝을 위한 제로 터치 컨피그레이션입니다.데이터 프레임에 대한 개인 정보 및 인증네트워크와 노드 간의 상호 인증.실내 메시 AP 노드 인증에 표준 EAP 방법을 사용할 수 있습니다.LWAPP 및 실내 메시 보안 분리검색, 라우팅 및 동기화 메커니즘이 현재 아키텍처에서 향상되어 새로운 보안 프로토콜을 지원하는 데 필요한 요소를 수용합니다.실내 메시 AP는 다른 메시 AP에서 불필요한 네이버 업데이트를 검색하고 수신하여 다른 메시 AP를 검색합니다.네트워크에 연결된 모든 RAP 또는 실내 MAP은 NEIGH_UPD 프레임(802.11 비컨 프레임과 유사)에서 코어 보안 매개변수를 광고합니다.이 단계가 끝나면 실내 메시 AP와 루트 AP 간의 논리적 링크가 설정됩니다.
- **WCS 개선 사항**실내 메시 경보가 추가되었습니다.홉수, 최악의 SNR 등을 보여주는 실내 메시 보고서를 생성할 수 있습니다.링크 테스트(Parent-to-Child, Child-to-Parent)는 매우 지능적인 정보를 표시하는 노드 간에 실행할 수 있습니다.표시되는 AP 정보는 이전 정보보다 훨씬 많습니다.잠재적 인접 디바이스도 볼 수 있습니다.상태 모니터링이 개선되고 더 편리하게 액세스할 수 있습니다.

지원되는 하드웨어 및 소프트웨어

실내 메쉬에는 최소 하드웨어 및 소프트웨어 요구 사항이 있습니다.

- Cisco LWAPP AP AIR-LAP1242AG-A-K9 및 AIR-LAP1131AG-A-K9는 실내 메시 컨피그레이션을 지원합니다.
- Cisco Mesh Release 2 소프트웨어는 Enterprise Mesh(실내 및 실외 제품)를 지원합니다. Cisco 컨트롤러, Cisco 440x/210x 및 WISM에만 설치할 수 있습니다.
- Cisco Enterprise Mesh Release 2 소프트웨어는 Cisco.com에서 다운로드할 수 있습니다.

실내 대 실외

다음은 실내 메쉬와 실외 메시 간의 핵심적인 차이점입니다.

	실내 메시	**실외 메시**
환경	실내 전용, 하드웨어 실내 등급	실외 전용, 견고한 하드웨어
하드웨어	LAP1242 및 LAP1131AG를 사용	LAP15xx 및 LAP152x를 사용하

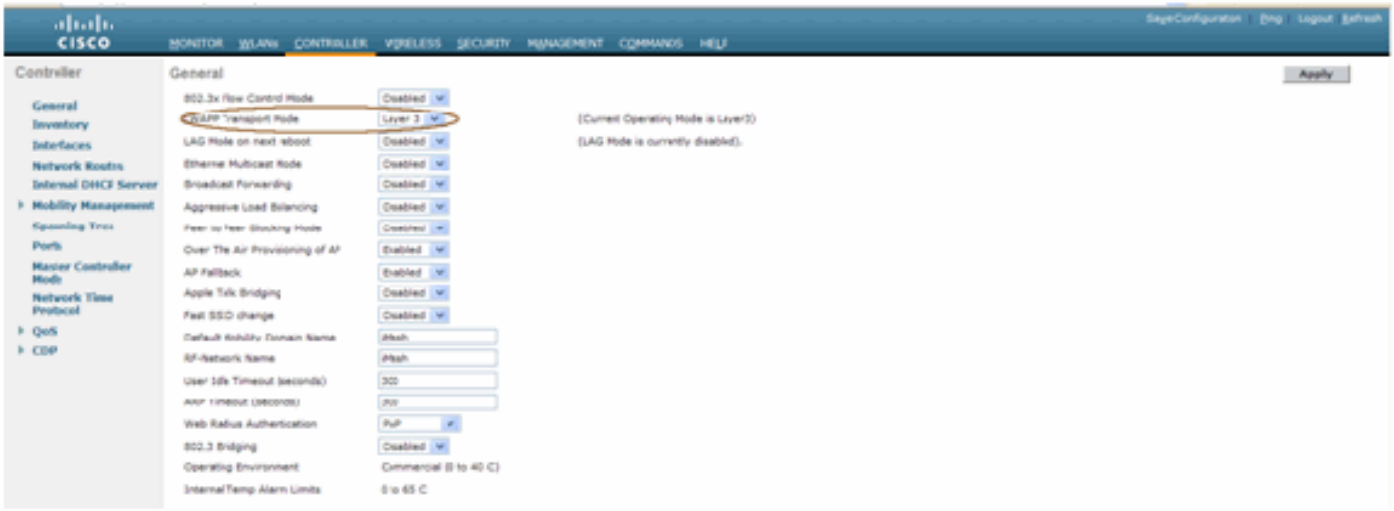
	하는 실내 AP	는 실외 AP
전력 레벨	2.4Ghz:20dbm 5.8Ghz:17dbm	2.4Ghz:28dbm 5.8Ghz:28dbm
셀 크기	약 150피트	약 1000피트
구현 높이	지면에서 12피트	30-40피트(지상)

구성

구현을 시작하기 전에, 특히 새 하드웨어를 받은 경우 설명서를 철저히 검토하십시오.

컨트롤러 L3 모드

실내 메시 AP는 L3 네트워크로 구축할 수 있습니다.



컨트롤러를 최신 코드로 업그레이드

다음 단계를 완료하십시오.

1. 실내 메시 네트워크에서 Mesh Release 2를 업그레이드하려면 Cisco.com에서 사용 가능한 4.1.185.0 또는 Mesh Release1에서 네트워크가 실행되고 있어야 합니다.
2. 컨트롤러에 대한 최신 코드를 TFTP 서버에 다운로드합니다.Controller GUI 인터페이스에서 Commands(**명령**) > **Download file(파일 다운로드)을** 클릭합니다.
3. File type as **code를** 선택하고 TFTP 서버의 IP 주소를 지정합니다.파일의 경로와 이름을 정의합니다

.

참고: 32MB 이상의 파일 크기 전송을 지원하는 TFTP 서버를 사용합니다.예를 들어 tftpd**32**.

파일 경로 아래에 표시된 대로 "./"를 입력합니다.

4. 새 펌웨어 설치가 완료되면 CLI에서 **show sysinfo** 명령을 사용하여 새 펌웨어가 설치되었는지 확인합니다

.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.....................................
System Contact......................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

참고: 공식적으로 Cisco는 컨트롤러에 대한 다운그레이드를 지원하지 않습니다.

MAC 주소

MAC 필터링을 사용해야 합니다.이 기능을 통해 Cisco 실내 메시 솔루션은 진정한 "제로 터치(Zero Touch)"가 되었습니다. 이전 릴리스와 달리 메시 화면에는 더 이상 MAC 필터링 옵션이 없습니다.

참고: MAC 필터링은 기본적으로 활성화되어 있습니다.

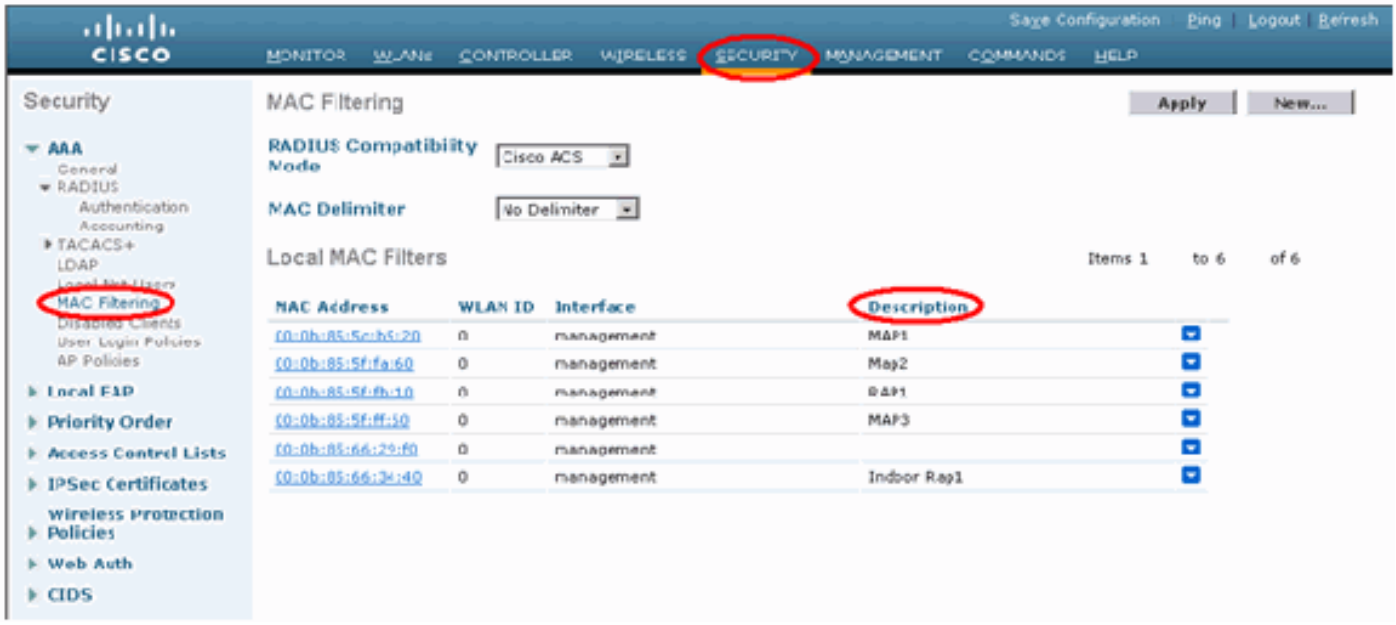
무선에 MAC 주소 기록

텍스트 파일에서 네트워크에 구축하는 모든 실내 메시 AP 무선 장치의 MAC 주소를 기록합니다 .MAC 주소는 AP 뒷면에서 찾을 수 있습니다.대부분의 CLI 명령에서 명령을 사용하여 AP MAC 주소 또는 이름을 입력해야 하므로 이를 통해 나중에 테스트할 수 있습니다.AP의 이름을 "building number-pod number-AP type:마지막 4개의 MAC 주소 16진수 문자."

컨트롤러에서 MAC 주소 및 무선 이름 입력

Cisco 컨트롤러는 실내 AP 권한 부여 MAC 주소 목록을 유지 관리합니다.컨트롤러는 권한 부여 목록에 나타나는 실내 무선 장치의 검색 요청에만 응답합니다.컨트롤러의 네트워크에서 사용하는 모든 무선 장치의 MAC 주소를 입력합니다.

컨트롤러 GUI 인터페이스에서 **Security(보안)**로 이동하고 화면 왼쪽**에서 MAC 필터링**을 클릭합니다.**New(새로** 만들기)를 클릭하여 다음과 같이 MAC 주소를 입력합니다.



또한 **설명**에 편의를 위해 무선 장치 이름(예: 위치, AP 번호 등)을 입력합니다. 또한 언제든지 쉽게 참조할 수 있도록 무선 장치가 설치된 위치에도 설명을 사용할 수 있습니다.

MAC 필터링 활성화

MAC 필터링은 기본적으로 활성화되어 있습니다.

또한 동일한 페이지에서 보안 모드를 EAP 또는 PSK로 선택할 수 있습니다.

스위치의 GUI 인터페이스에서 다음 경로를 사용합니다.

GUI 인터페이스 경로:**무선 > 실내 메시**

보안 모드는 CLI에서만 다음 명령을 통해 확인할 수 있습니다.

```
(Cisco Controller) > show network
```

```
(Cisco Controller) >show network

RF-Network Name.............................. iMesh
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Mode...................... Disable   Mode: Ucast
Ethernet Broadcast Mode...................... Disable
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
ARP Unicast Mode............................. Disabled
Cisco AP Default Master...................... Disable
Mgmt Via Wireless Interface.................. Disable
Mgmt Via Dynamic Interface................... Disable
Bridge MAC filter Config..................... Enable
Bridge Security Mode......................... EAP
Mesh Multicast Mode.......................... 802.11b/g/n
Mesh Full Sector DFS......................... Enable
Over The Air Provisioning of AP's............ Enable
Mobile Peer to Peer Blocking................. Disable
Apple Talk .................................. Disable
AP Fallback ................................. Enable
--More-- or (q)uit
Web Auth Redirect Ports ..................... 80
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

L3 실내 메시 구축

L3 실내 메시 네트워크의 경우 DHCP 서버(내부 또는 외부)를 사용하지 않으려는 경우 무선 장치의 IP 주소를 구성합니다.

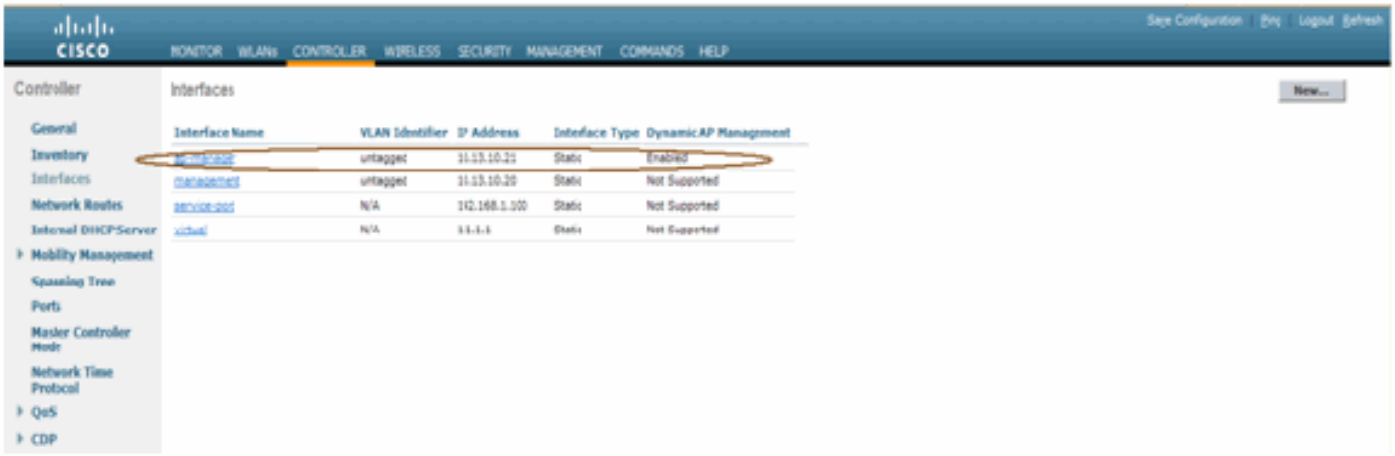
L3 실내 메시 네트워크의 경우 DHCP 서버를 사용하려면 L3 모드에서 컨트롤러를 구성합니다.컨피그레이션을 저장하고 컨트롤러를 재부팅합니다.DHCP 서버에서 옵션 43을 구성해야 합니다.컨트롤러가 다시 시작된 후 새로 연결된 AP는 DHCP 서버에서 IP 주소를 받습니다.

컨트롤러에서 인터페이스 정의

AP 관리자

L3 구축의 경우 **AP-관리자**를 정의해야 합니다.AP 관리자는 컨트롤러에서 AP로의 통신을 위한 소스 IP 주소 역할을 합니다.

경로:**Controller(컨트롤러) > Interfaces(인터페이스) > ap-manager > edit(수정)**.



AP **관리자** 인터페이스에는 관리 인터페이스와 동일한 서브넷 및 VLAN의 IP 주소가 할당되어야 합니다.

무선 역할

이 솔루션에는 두 가지 기본 라디오 역할이 있습니다.

- RAP(Root Access Point) - 스위치를 통해 컨트롤러에 연결하려는 라디오가 RAP 역할을 수행

합니다.RAP는 컨트롤러에 대한 유선 LWAPP 지원 연결을 가집니다.RAP는 브리징 또는 실내 메시 네트워크의 상위 노드입니다.컨트롤러는 하나 이상의 RAP를 가질 수 있으며, 각 RAP는 동일하거나 다른 무선 네트워크를 둘 수 있습니다.이중화를 위해 동일한 실내 메시 네트워크에 대해 둘 이상의 RAP가 있을 수 있습니다.

- 실내 메시 액세스 포인트(MAP) - 컨트롤러와 유선 연결이 없는 라디오는 실내 메시 AP의 역할을 합니다.이 AP는 이전에 Pole top AP라고 불렸습니다.MAP는 다른 MAP에 대한 무선 연결(백홀 인터페이스를 통해)을 가지며, 마지막으로 RAP에 연결하여 컨트롤러에 연결합니다.MAP는 LAN에 유선 이더넷 연결을 가질 수도 있으며 P2P 또는 P2MP 연결을 사용하여 해당 LAN에 대한 브리지 엔드포인트 역할을 합니다. 이더넷 브리지로 올바르게 구성된 경우 동시에 발생할 수 있습니다.백홀 인터페이스에 사용되지 않는 밴드의 MAP 서비스 클라이언트

AP의 기본 모드는 MAP입니다.

참고: 라디오 역할은 GUI 또는 CLI를 통해 설정할 수 있습니다.역할 변경 후 AP가 재부팅됩니다.

참고: AP가 스위치에 물리적으로 연결되어 있거나 스위치의 AP를 RAP 또는 MAP로 볼 수 있는 경우 컨트롤러 CLI를 사용하여 AP에서 라디오 역할을 미리 구성할 수 있습니다.

```
(Cisco Controller) >config ap role ?

rootAP          RootAP role for the Cisco Bridge.
meshAP          MeshAP role for the Cisco Bridge.

(Cisco Controller) >config ap role meshAP ?

<Cisco AP>      Enter the name of the Cisco AP.

(Cisco Controller) >config ap role meshAP LAP1242-2

Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

브리지 그룹 이름

BGN(Bridge Group Names)은 AP의 연결을 제어합니다.BGN은 동일한 채널에 있는 두 네트워크가 서로 통신하지 않도록 라디오를 논리적으로 그룹화할 수 있습니다.이 설정은 네트워크에 동일한 섹터(영역)에 둘 이상의 RAP가 있는 경우에도 유용합니다. BGN은 최대 10자의 문자열입니다.

제조 단계(NULL VALUE)에 공장 세트 브리지 그룹 이름이 지정됩니다. 보이지 않습니다.따라서 정의된 BGN이 없어도 무선 장치가 네트워크에 계속 연결될 수 있습니다.네트워크에 같은 섹터에 두 개의 RAP가 있는 경우(더 많은 용량을 위해) 두 RAP를 동일한 BGN으로 구성하는 것이 좋지만 다른 채널에서 구성하는 것이 좋습니다.

참고: 브리지 그룹 이름은 컨트롤러 CLI 및 GUI에서 설정할 수 있습니다.

```
(Cisco Controller) >config ap bridgegroupname set ?

<bridgegroupname> Set bridgegroupname on Cisco AP.
```

BGN을 구성한 후 AP가 재설정됩니다.

참고: BGN은 라이브 네트워크에서 매우 신중하게 구성해야 합니다.항상 가장 먼 노드(마지막 노드)에서 시작하여 RAP로 이동해야 합니다.이유는 멀티홉의 중간에 BGN을 구성하기 시작하면 해당 노드에 다른 BGN(이전 BGN)이 있으므로 이 지점 이후의 노드가 삭제됩니다.

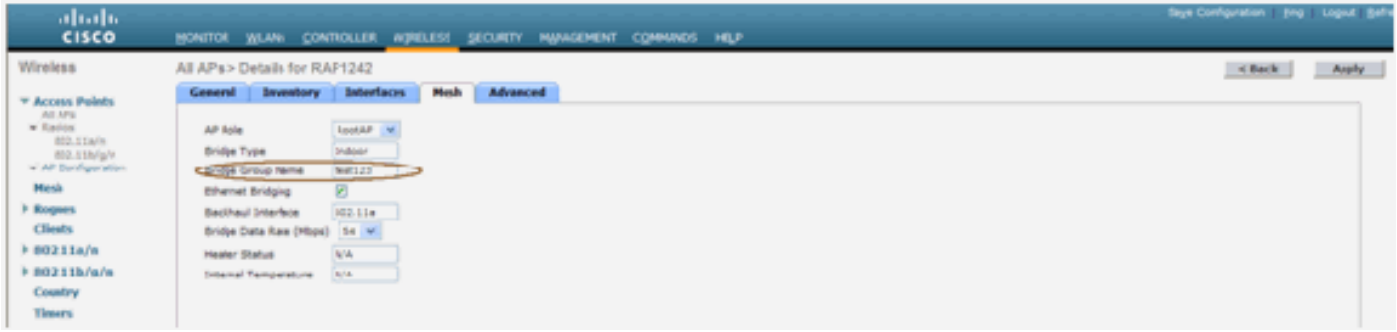
다음 CLI 명령을 실행하여 BGN을 확인할 수 있습니다.

(Cisco Controller) **> show ap config general**

```
(Cisco Controller) >show ap config general RAP1242

Cisco AP Identifier.............................. 0
Cisco AP Name.................................... RAP1242
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:18:74:fa:7d:1f
IP Address Configuration......................... DHCP
IP Address....................................... 10.13.13.11
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.13.13.10
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch............................. J2106-1
Secondary Cisco Switch...........................
Tertiary Cisco Switch............................
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Bridge
--More-- or (q)uit
AP Role ......................................... RootAP
Ethernet Bridging ............................... Enabled
Bridge GroupName ................................ test123
Public Safety ..................................  Disabled
Remote AP Debug ................................. Disabled
S/W  Version .................................... 4.1.175.19
Boot  Version ................................... 12.3.7.1
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Disabled
PoE Power Injector MAC Addr...................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
IOS Version...................................... 12.4(20070808:082741)
Reset Button..................................... Enabled
AP Serial Number................................. FTX1035B3RH
AP Certificate Type.............................. Manufacture Installed
Management Frame Protection Validation.......... Disabled
Console Login Name...............................
Console Login State.............................. Unknown
AP Up Time....................................... 0 days, 02 h 43 m 38 s
AP LWAPP Up Time................................. 0 days, 02 h 42 m 43 s
--More-- or (q)uit
Join Date and Time............................... Sun Aug 19 11:59:07 2007

Join Taken Time.................................. 0 days, 00 h 00 m 24 s
Ethernet Port Duplex............................. Unknown
Ethernet Port Speed.............................. Unknown
```

또한 컨트롤러 GUI를 사용하여 BGN을 구성하거나 확인할 수 있습니다.

경로:**무선 > 모든 AP > 세부사항**.



이 새 릴리스와 함께 AP의 환경 정보도 표시됩니다.

보안 구성

기본 실내 메시 보안 모드는 EAP입니다.즉, 컨트롤러에서 이러한 매개변수를 구성하지 않으면 MAP이 조인되지 않습니다.

실내 메시 EAP 컨피그레이션 CLI

```
(Cisco Controller) >config mesh local-auth enable

 enable Local Auth

(Cisco Controller) >config advanced eap ?

identity-request-timeout Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries Configures EAP-Identity-Request Max Retries.
key-index      Configure the key index used for dynamic WEP (802.1x) unicast key (PTK).
max-login-ignore-identity-response Configure to ignore the same username count reaching max in the E
AP identity response
request-timeout Configures EAP-Request Timeout in seconds.
request-retries Configures EAP-Request Max Retries.
```

PSK 모드를 유지해야 하는 경우 다음 명령을 사용하여 PSK 모드로 돌아갑니다.

```
(Cisco Controller) >config mesh security psk ?

(Cisco Controller) >config mesh security psk

 All Mesh AP will be rebooted
 Are you sure you want to start? (y/N)n
```

실내 메시 EAP show 명령

EAP 모드 내에서 다음 **show** 명령을 확인하여 MAP 인증을 확인할 수 있습니다.

```
(Cisco Controller) >show network

RF Network Name............................... jaggi123
Web Mode...................................... Disable
Secure Web Mode............................... Enable
Secure Shell (ssh)............................ Enable
Telnet........................................ Enable
Ethernet Multicast Mode....................... Disable   Mode: Mcast  224.1.1.1
Ethernet Broadcast Mode....................... Disable
User Idle Timeout............................. 300 seconds
ARP Idle Timeout.............................. 300 seconds
ARP Unicast Mode.............................. Disabled
Cisco AP Default Master....................... Disable
Mgmt Via Wireless Interface................... Enable
Mgmt Via Dynamic Interface.................... Disable
Bridge MAC filter Config...................... Disable
Bridge Security Mode.......................... EAP  otherwise PSK
Mesh Multicast Mode........................... 802.11b/g/n
Mesh Full Sector DFS.......................... Enable
Over The Air Provisioning of AP's............. Enable
Mobile Peer to Peer Blocking.................. Disable
AP Fallback .................................. Enable
Web Auth Redirect Ports ...................... 80
--More-- or (q)uit
Fast SSID Change ............................. Disabled
802.3 Bridging ............................... Disable
```

(Cisco Controller) >**show wlan 0**

```
(Cisco Controller) >show wlan 0

WLAN Identifier.................................. 0
Profile Name..................................... Mesh_profile
Network Name (SSID).............................. Mesh_ssid
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 2
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Allowed
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All
Local EAP Authentication......................... Enabled (Profile 'prfMaP1500LlEAuth93')
Security

   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
                                                  Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Disabled
   CKIP ..........................................Disabled
   IP Security Passthru.......................... Disabled
   Web Based Authentication...................... Disabled
   Web-Passthrough............................... Disabled
   Conditional Web Redirect...................... Disabled
   Auto Anchor................................... Disabled
--More-- or (q)uit
   H-REAP Local Switching........................ Disabled
   Infrastructure MFP protection................. Enabled (Global Infrastructure MFP Disabled)
   Client MFP.................................... Optional
   Tkip MIC Countermeasure Hold-down Timer....... 60

 Mobility Anchor List
 WLAN ID       IP Address        Status
```

(Cisco Controller) >**show local-auth config**

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout .............................. 300

Configured EAP profiles:

EAP Method configuration:
    EAP-FAST:
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Authority ID .............................. 436973636f0000000000000000000000
      Authority Information ..................... Cisco A-ID

(Cisco Controller) >show advanced eap


EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries........... 20
EAP Key-Index for Dynamic WEP.............. 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds).............. 1
EAP-Request Max Retries.................... 2
```

```
(Cisco Controller) >show advanced eap
```

실내 메시 EAP 디버그 명령

EAP 모드 문제를 디버깅하려면 컨트롤러에서 다음 명령을 사용합니다.

```
(Cisco Controller) >debug dot1x all enable

(Cisco Controller) >debug aaa all enable
```

설치

전제 조건

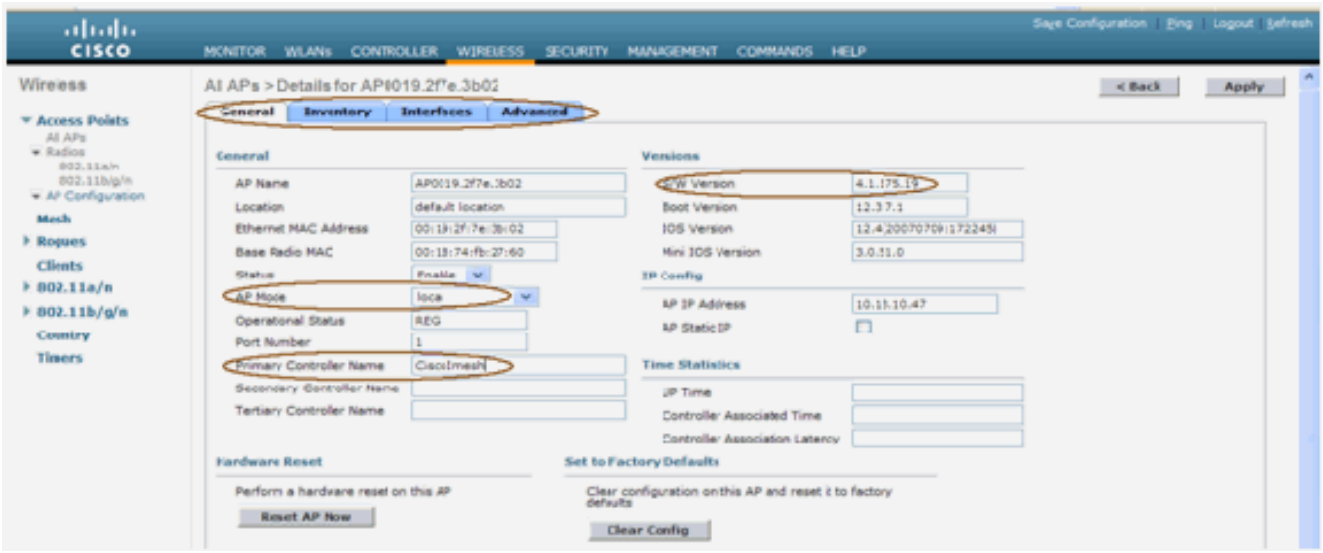
컨트롤러에서 권장 버전의 코드를 실행해야 합니다.Monitor(**모니터링**)를 클릭하여 소프트웨어 버전을 확인합니다.CLI를 통해 동일한 내용을 확인할 수 있습니다.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.....................................
System Contact......................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

DHCP 서버, ACS 서버 및 WCS 서버와 같은 시스템에 연결할 수 있어야 합니다.

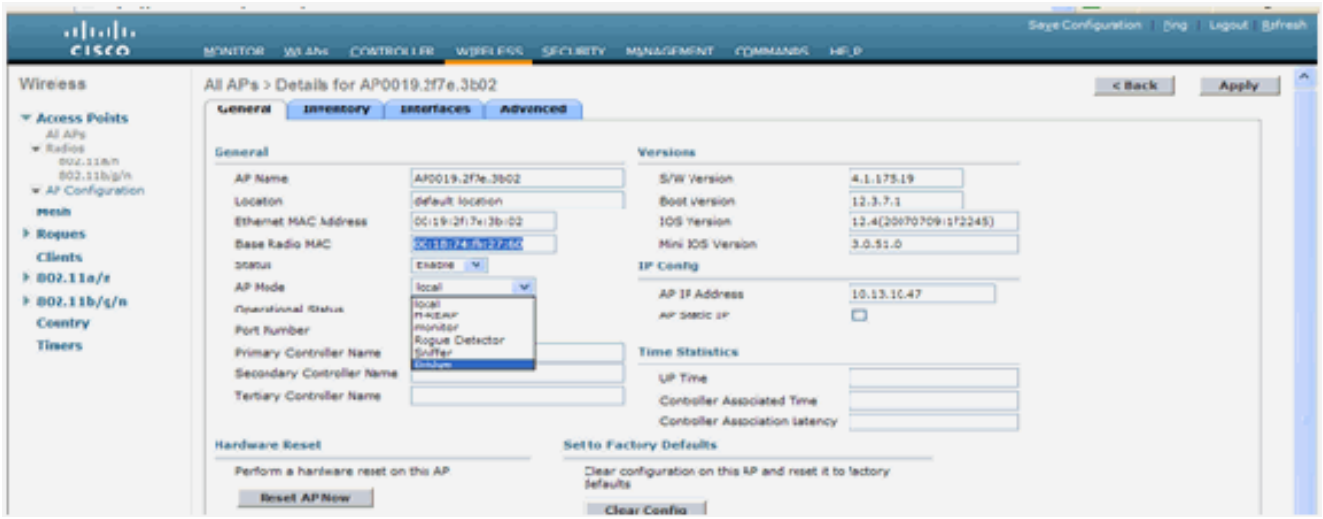
설치

1. 모든 LAP(1131AG/1242AG)를 관리 IP 주소와 동일한 서브넷의 레이어 3 네트워크에 연결합니다.모든 AP가 로컬 모드에서 AP로 컨트롤러에 연결됩니다.이 모드에서는 기본 컨트롤러 이름, 보조 컨트롤러 이름 및 3차 컨트롤러 이름으로 AP를 우선시합니다
   .



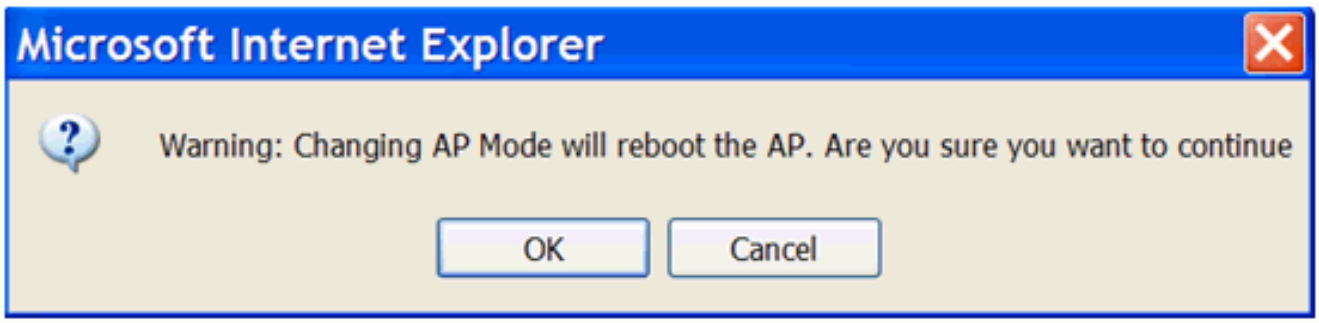
2. AP의 기본 라디오 MAC 주소를 캡처합니다(예: 00:18:74:fb:27시 60분)
3. 브리지 모드에서 AP에 연결할 AP의 MAC 주소를 추가합니다.
4. Security(**보안**) > **MAC-filtering(MAC 필터링)** > New(**새로 만들기)를 클릭합니다**.
5. 복사된 MAC 주소를 추가하고 MAC-filter 목록 및 AP 목록에서 AP의 이름을 지정합니다.
6. **AP Mode** 목록에서 Bridge를 선택합니다

.



7. 그러면 AP가 리부팅되므로 확인 메시지가 표시됩니다

.



8. AP가 재부팅되고 브리지 모드에서 컨트롤러에 조인됩니다.새 AP 창에는 추가 탭이 있습니다 .메시MESH 탭을 클릭하여 역할, 브리지 유형, 브리지 그룹 이름, 이더넷 브리징, 백홀 인터페이스, 브리지 데이터 속도 등을 확인합니다

.

9. 이 창에서 AP 역할 목록에 액세스하여 관련 역할을 선택합니다.이 경우 기본적으로 역할은 MAP입니다.브리지 그룹 이름은 기본적으로 비어 있습니다.백홀 인터페이스는 802.11a입니다.브리지 데이터 속도(즉, 백홀 데이터 속도)는 24Mbps입니다.
10. RAP로 사용할 AP를 컨트롤러에 연결합니다.원하는 위치에 라디오(MAP)를 구축합니다.라디오를 켜라.컨트롤러의 모든 라디오를 볼 수 있어야 합니다

.

```
(Cisco Controller) >show ap summ

Number of APs.................................... 3

AP Name             Slots  AP Model             Ethernet MAC       Location          Port  Country
-----------------   -----  -------------------  -----------------  ----------------  ----  -------
RAP1242             2      AIR-LAP1242AG-A-K9   00:18:74:fa:7d:1f  default location  1     US
LAP1242-1           2      AIR-LAP1242AG-A-K9   00:1b:2b:a7:ad:bf  default location  1     US
LAP1242-2           2      AIR-LAP1242AG-A-K9   00:14:1b:59:07:af  default location  1     US
```

11. 노드 간에 가시성 조건을 설정해 보십시오.LOB(line-of-sight) 조건이 없으면 Fresnel zone clearance를 생성하여 LOB(Near-Line-of-Site) 조건을 가져옵니다.
12. 동일한 실내 메시 네트워크에 두 개 이상의 컨트롤러가 연결된 경우 모든 노드에서 기본 컨트롤러의 이름을 지정해야 합니다.그렇지 않으면 먼저 보이는 컨트롤러가 기본으로 사용됩니다.

전원 및 채널 구성

백홀 채널은 RAP에서 구성할 수 있습니다.MAP은 RAP 채널에 맞게 조정됩니다.로컬 액세스는 MAP에 대해 독립적으로 구성할 수 있습니다.

스위치 GUI에서 경로를 따릅니다.**무선 > 802.11a 라디오 > 구성**.

참고: 백홀의 기본 Tx 전력 레벨은 최고 전력 레벨(레벨 1)이고 RRM(Radio Resource Management)은 기본적으로 꺼집니다.

RAP를 병합하는 경우 각 RAP에서 대체 인접 채널을 사용하는 것이 좋습니다.따라서 공동 채널 간섭이 줄어듭니다.

RF 확인

실내 메시 네트워크에서는 노드 간의 모-자 관계를 확인해야 합니다.**Hop**은 두 무선 통신 간의 무선 링크입니다.네트워크를 통해 이동할 때 상위-하위 관계가 변경됩니다.실내 메시 네트워크의 위치에 따라 달라집니다.

무선 연결(hop)에서 컨트롤러에 더 가까운 라디오는 홉의 반대쪽에 있는 라디오의 부모입니다.다중 hop 시스템에는 컨트롤러에 연결된 노드가 RAP(**Parent**)인 트리 유형 구조가 있습니다. 첫 번째 홉의 다른 쪽에 있는 직속 노드는 **하위 노드이며**, 두 번째 홉의 후속 노드는 해당 특정 상위의 **인접** 노드입니다.

그림 1:2홉의 네트워크

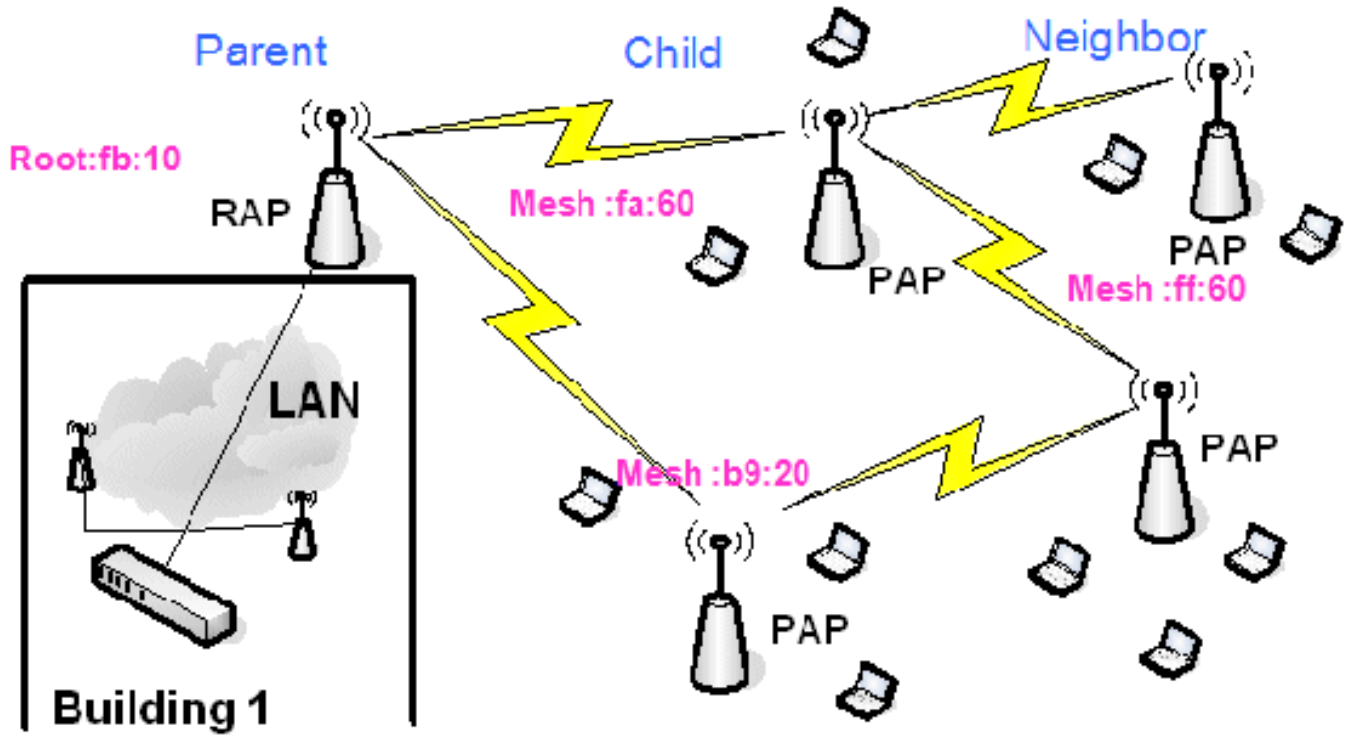


그림 1에서 편리하게 AP 이름을 언급합니다.다음 스크린샷에서 **RAP(fb:10)**를 조사하고 있습니다.이 노드는 실내 메시 AP**(fa:60 & b9:20)**를 자**로, MAP ff:60을 인접 디바이스로** 볼 수 있습니다.

스위치 GUI 인터페이스에서 경로를 따릅니다.**무선 > 모든 AP > Rap1 > 인접 디바이스 정보**.

실내 메시 네트워크에 대해 모-자 관계(Parent-Child Relations)가 올바르게 설정되고 유지되는지 확인합니다.

상호 연결 확인

show Mesh는 네트워크의 상호 연결을 확인하는 정보 명령입니다.

컨트롤러 CLI를 사용하여 각 노드(AP)에서 이러한 명령을 제공하고 결과를 Word 또는 텍스트 파일로 업로드 사이트에 업로드해야 합니다.

```
(Cisco Controller) >show mesh ?

env             Show mesh environment.
neigh           Show AP neigh list.
path            Show AP path.
stats           Show AP stats.
secbh-stats     Show Mesh AP secondary backhaul stats.
per-stats       Show AP Neighbor Packet Error Rate stats.
queue-stats     Show AP local queue stats.
security-stats  Show AP security stats.
config          Show mesh configurations.
secondary-backhaul Show mesh secondary-backhaul
client-access   Show mesh backhaul with client access.
public-safety   Show mesh public safety.
background-scanning Show mesh background-scanning state.
cac             Show mesh cac.
```

실내 메시 네트워크에서 여러 hop 링크를 선택하고 RAP부터 이 명령을 실행합니다.명령 결과를 업로드 사이트에 업로드합니다.

다음 섹션에서는 그림 1에 나와 있는 Two Hop Indoor Mesh Network에 대해 이러한 모든 명령이 실행되었습니다.

실내 메시 경로 표시

이 명령은 MAC 주소, 노드의 무선 역할, 업링크/다운링크의 dBs(SNRUp, SNRDown) 및 특정 경로의 dB의 링크 SNR을 보여줍니다.

```
(Cisco Controller) >show mesh path RAP1242

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
RAP1242           is a Root AP.
(Cisco Controller) >show mesh path LAP1242-2

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-1           56      29     29       27       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242             56      41     32       34       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242           is a Root AP.
```

실내 메시 네이버 요약 표시

이 명령은 dB의 MAC 주소, 상위-하위 관계 및 업링크/다운링크 SNR을 보여줍니다.

```
(Cisco Controller) >show mesh neigh ?

detail          Show Link rate neigh detail.
summary         Show Link rate neigh summary.
(Cisco Controller) >show mesh neigh  summary RAP1242

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      0      0        0        0x860    BEACON
LAP1242-1           56      0      33       0        0x960    CHILD BEACON


(Cisco Controller) >show mesh neigh  summary LAP1242-1

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      30     29       28       0x961    UPDATED CHILD BEACON
RAP1242             56      43     46       31       0x86b    UPDATED NEIGH PARENT BEACON
```

이때 네트워크의 노드 간의 관계를 확인하고 모든 링크의 SNR 값을 확인하여 RF 연결을 확인할 수 있어야 합니다.

AP 콘솔 액세스 보안

이 기능은 AP의 콘솔 액세스에 대한 보안을 강화합니다.이 기능을 사용하려면 AP용 콘솔 케이블이 필요합니다.

지원되는 항목은 다음과 같습니다.

- 사용자 ID/비밀번호 조합을 지정된 AP에 푸시하는 CLI:

```
(Cisco Controller) >config ap username Cisco password Cisco ?

all             Configures the Username/Password for all connected APs.
<Cisco AP>      Enter the name of the Cisco AP.
```

- 컨트롤러에 등록된 모든 AP에 사용자 이름/비밀번호 조합을 푸시하는 CLI 명령 :

```
(Cisco Controller) >config ap username Cisco password Cisco all
```

이러한 명령을 사용하면 컨트롤러에서 푸시된 사용자 ID/비밀번호 조합이 AP의 다시 로드 전반에 걸쳐 지속됩니다.컨트롤러에서 AP가 지워지면 보안 액세스 모드가 없습니다.AP는 성공적으로 로그인하여 SNMP 트랩을 생성합니다.또한 AP는 콘솔 로그인 실패 시 3회 연속 SNMP 트랩을 생성합니다.

이더넷 브리징

보안상의 이유로 MAP의 이더넷 포트는 기본적으로 비활성화되어 있습니다.RAP와 각 MAP에 이더넷 브리징을 구성해야만 활성화할 수 있습니다.

따라서 두 가지 시나리오에서 이더넷 브리징을 활성화해야 합니다.

- 실내 메시 노드를 브리지로 사용하려는 경우
- 이더넷 포트를 사용하여 MAP의 이더넷 장치(예: PC/랩톱, 비디오 카메라 등)를 연결하려는 경우

경로:**무선** > 임의의 AP > **메시**를 클릭합니다.

브리징을 수행하는 노드 간의 거리를 구성하는 데 사용할 수 있는 CLI 명령이 있습니다.모든 홉에서 비디오 카메라처럼 이더넷 장치를 연결하고 성능을 확인하십시오.

브리지 그룹 이름 향상

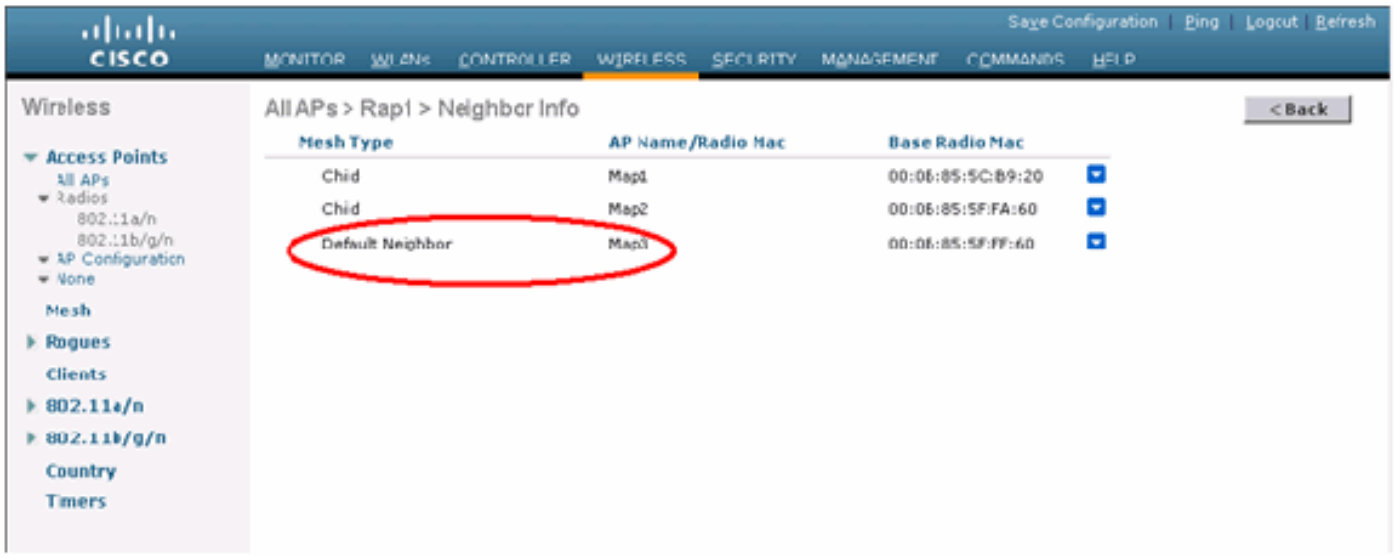
의도하지 않은 "bridgegroupname"으로 AP를 잘못 프로비저닝할 수 있습니다.네트워크 설계에 따라 이 AP는 연락하여 올바른 섹터/트리를 찾을 수 없거나 찾지 못할 수 있습니다.호환 가능한 부문에 연결할 수 없다면 오도가도 못하게 될 수 있다.

이러한 고립된 AP를 복구하기 위해 3.2.xx.x 코드와 함께 '기본' 브리지그룹 이름 개념을 도입했습니다.기본적으로 구성된 브리지그룹 이름으로 다른 AP에 연결할 수 없는 AP는 "default"(단어)를 브리지그룹 이름으로 연결하려고 시도합니다.3.2.xx.x 이상 소프트웨어를 실행하는 모든 노드는 이 브리지그룹 이름을 가진 다른 노드를 허용합니다.

이 기능은 실행 중인 네트워크에 새 노드 또는 잘못 구성된 노드를 추가하는 데에도 도움이 됩니다.

실행 중인 네트워크가 있는 경우 다른 BGN을 사용하여 미리 구성된 AP를 가져와 네트워크에 연결합니다.컨트롤러에서 MAC 주소를 추가한 후 "기본" BGN을 사용하여 컨트롤러에서 이 AP를 볼 수 있습니다.

```
(CiscoController) >show mesh path Map3:5f:ff:60

00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 4
8, linkSnr 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63,
 linkSnr 57
00:0B:85:5F:FB:10 is RAP
```



기본 BGN을 사용하는 AP는 클라이언트를 연결하고 실내 메시 상위 하위 관계를 형성하는 일반적인 실내 메시 AP의 역할을 할 수 있습니다.

기본 BGN을 사용하는 이 AP가 올바른 BGN이 있는 다른 부모를 찾는 순간 해당 BGN으로 전환됩니다.

로그 - 메시지, 시스템, AP 및 트랩

메시지 로그

메시지 로그에 대한 보고 레벨을 활성화합니다.컨트롤러 CLI에서 다음 명령을 실행합니다.

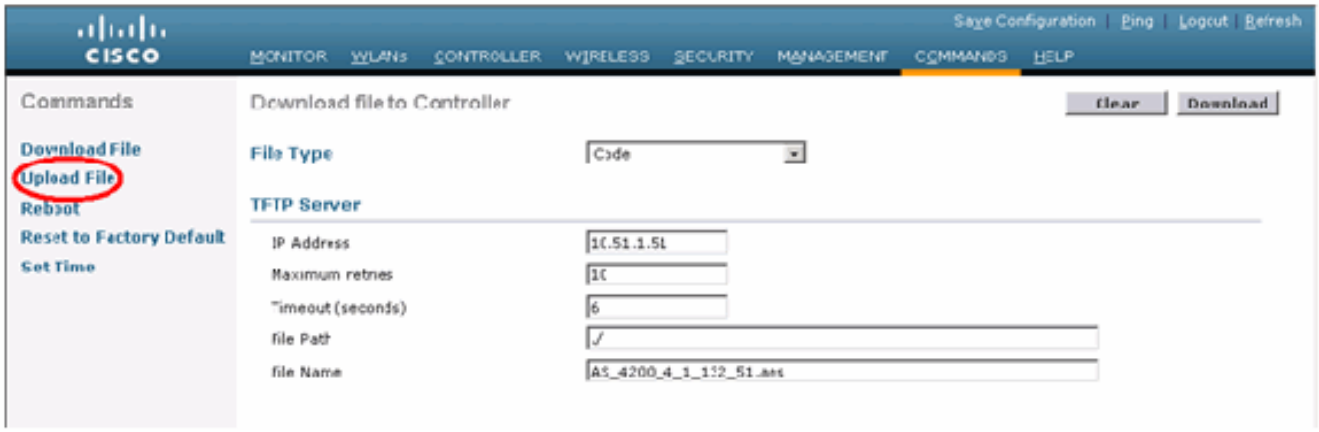
```
(Cisco Controller) >config msglog level ?

critical        Critical hardware or software Failure.
error           Non-Critical software error.
security        Authentication or security related error.
warning         Unexpected software events.
verbose         Significant system events.

(Cisco Controller) >config msglog level verbose
```

메시지 로그를 보려면 컨트롤러 CLI에서 다음 명령을 실행합니다.

```
(Cisco Controller) >show msglog

Message Log Severity Level ..................... VERBOSE
Mon Jul 11 01:42:08 2005  [SECURITY] apf_foreignap.c 765: Received a packet for
which no AP was configured from 00:0F:B5:93:71:E7 on port 0.
Fri Jul  8 06:12:02 2005  [ERROR] spam_radius.c 93: spamRadiusProcessResponse: A
P Authorization failure for 00:0b:85:0e:04:80
Fri Jul  8 05:40:15 2005  [ERROR] spam_tmr.c 501: Did not receive hearbeat reply
 from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:45 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:40 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:14:00
Fri Jul  8 05:38:40 2005  Previous message occurred 5 times
Fri Jul  8 05:33:54 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:32:23 2005  [ERROR] poe.c 449: poeInitPowerSupply : poePortResync
returned FAILURE.
Fri Jul  8 05:32:17 2005  [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Fri Jul  8 05:32:17 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11a swi
tch group reset
Fri Jul  8 05:32:16 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Fri Jul  8 05:32:16 2005  Previous message occurred 2 times
Fri Jul  8 05:31:19 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake cal
```

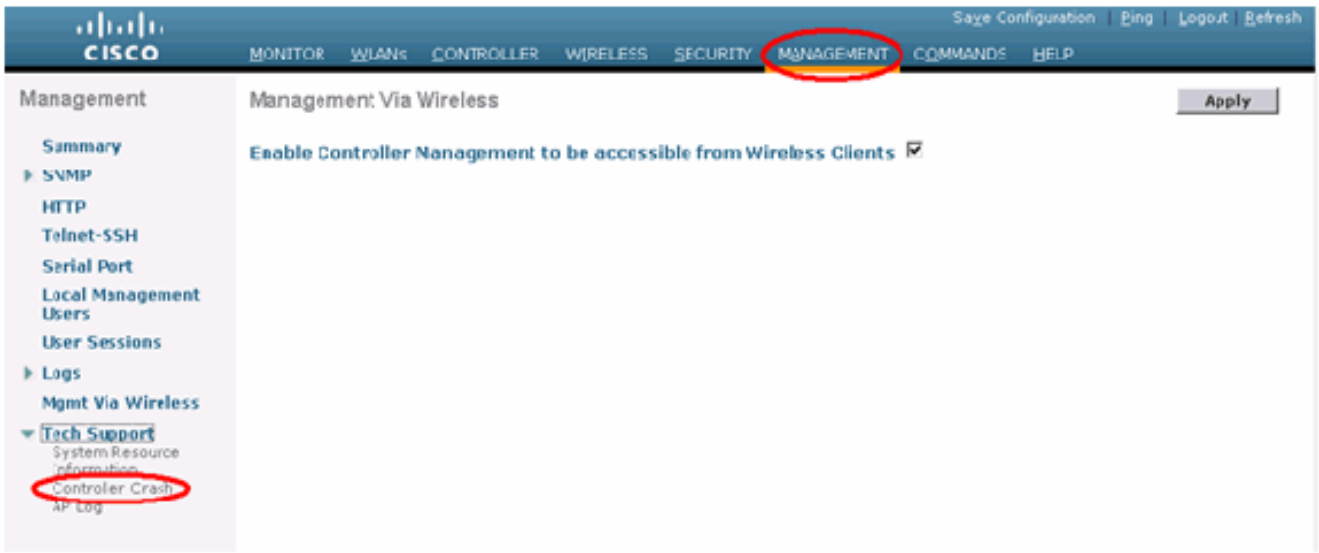
메시지 로그를 업로드하려면 컨트롤러 GUI 인터페이스를 사용합니다.

1. Commands(**명령**) > Upload(**업로드**)**를 클릭합니다**
   .



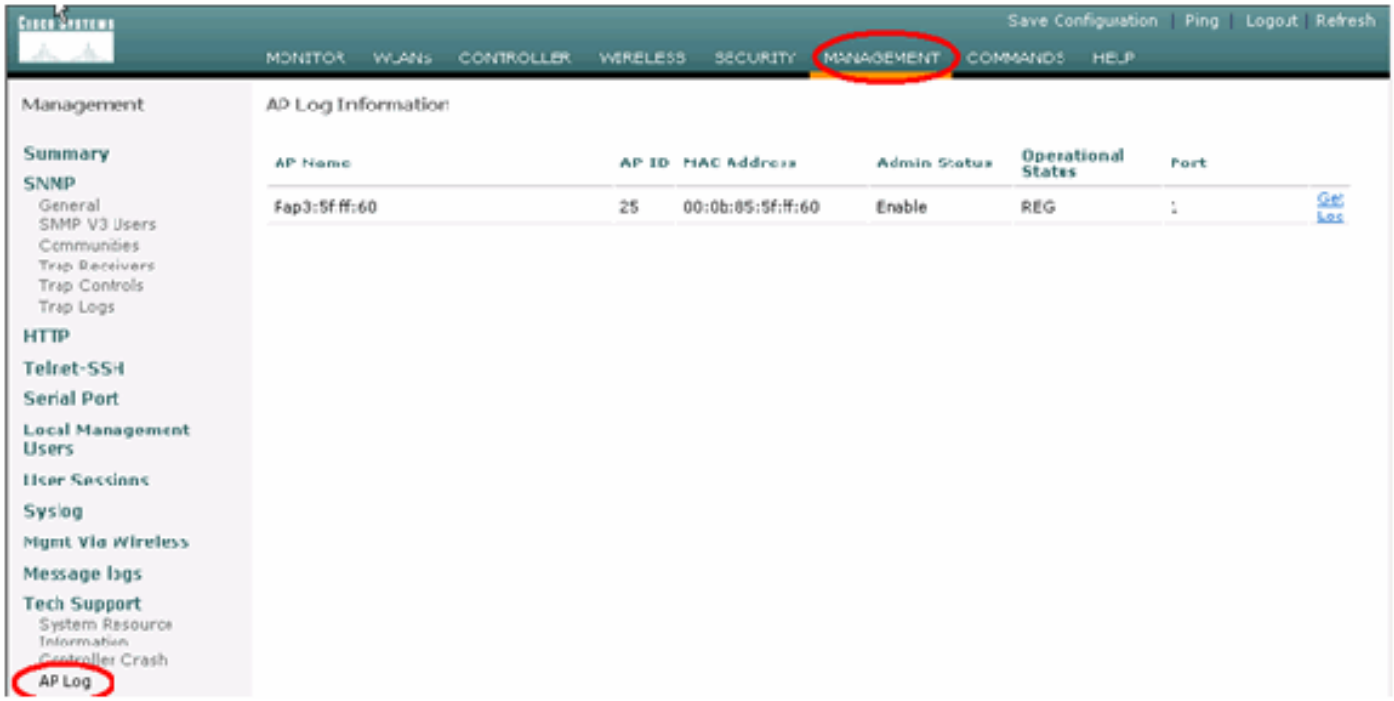
2. TFTP 서버 정보를 입력합니다.이 페이지에서는 업로드할 다양한 옵션을 제공하며 다음 파일을 전송하도록 합니다.메시지 로그이벤트 로그트랩 로그충돌 파일(있는 경우)Crash 파일을 확인하려면 **Management(관리) > Controller Crash(컨트롤러 충돌)를** 클릭합니다

.



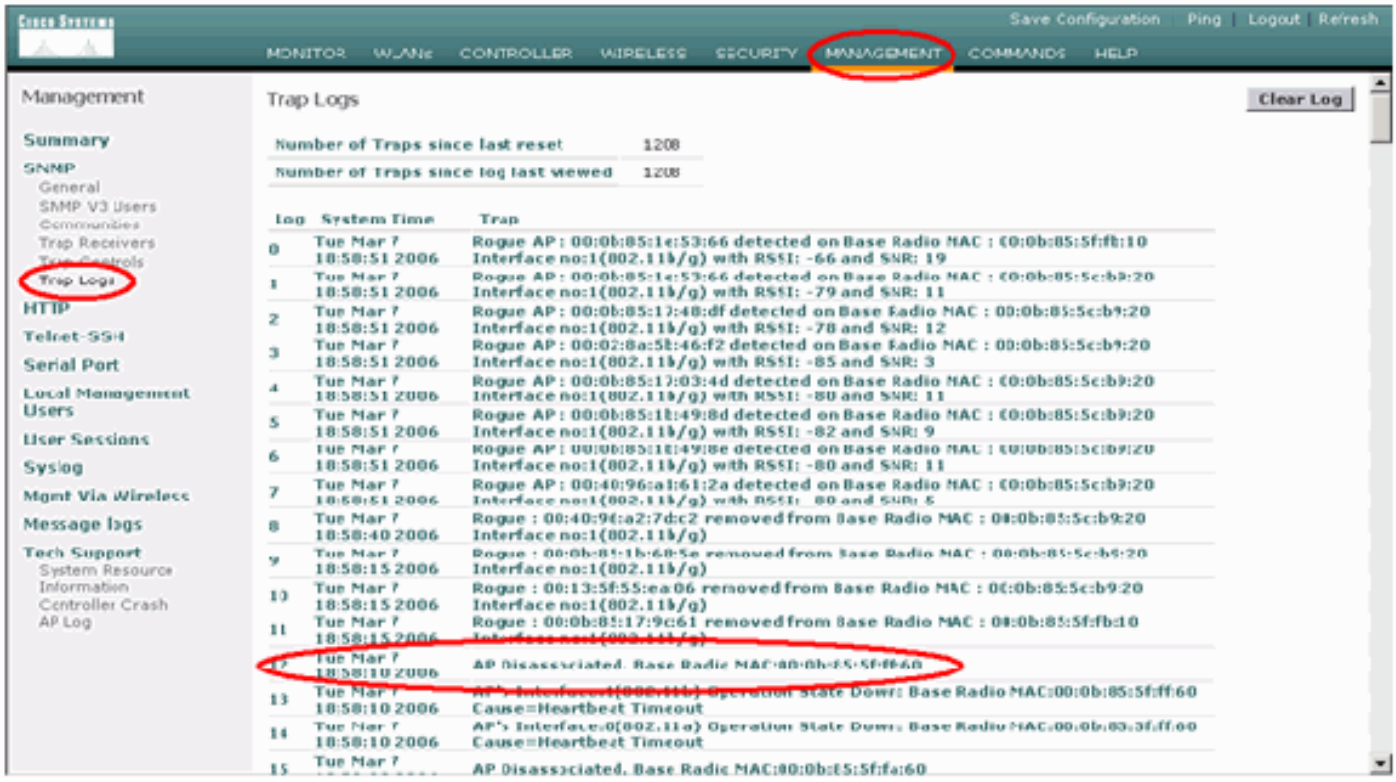
AP 로그

다음과 같은 경우 컨트롤러의 이 GUI 페이지로 이동하여 로컬 AP에 대한 AP 로그를 확인합니다.



트랩 로그

컨트롤러의 이 GUI 페이지로 이동하여 트랩 로그를 확인합니다.



성능

시작 통합 테스트

컨버전스는 RAP/MAP에서 WLAN 컨트롤러와의 안정적인 LWAPP 연결을 설정하는 데 걸리는 시간입니다. 이 시간은 WLAN 컨트롤러가 처음 부팅된 시점부터 여기에 나열된 대로 시작합니다.

통합 테스트	통합 시간(분:초)			
	RAP	맵1	맵2	맵3
이미지 업그레이드	2:34	3:50	5:11	6:38
컨트롤러 재부팅	0:38	0:57	1:12	1:32
실내 메시 네트워크 전원 켜기	2:44	3:57	5:04	6:09
RAP 재부팅	2:43	3:57	5:04	6:09
MAP 다시 조인		3:58	5:14	6:25
상위(동일한 채널)의 MAP 변경		0:38		

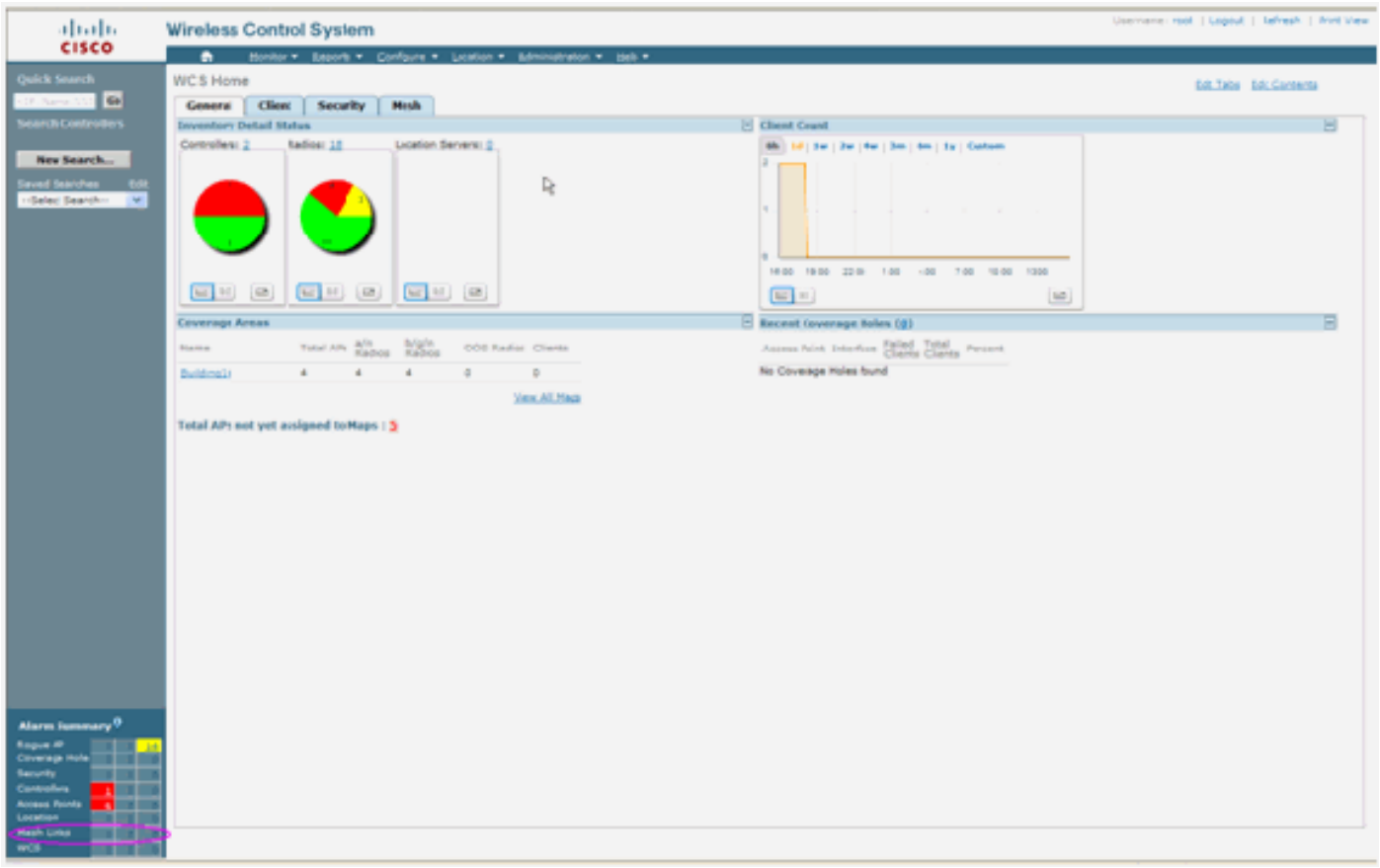
WCS

실내 메시 경보

WCS는 컨트롤러의 트랩을 기반으로 실내 메시 네트워크와 관련된 이러한 경보 및 이벤트를 생성합니다.

- 불량 링크 SNR
- 상위 변경됨
- 자식 이동됨
- 상위 항목을 자주 변경하는 MAP
- 콘솔 포트 이벤트
- MAC 권한 부여 실패
- 인증 실패
- 하위 제외 상위

메시 링크를 클릭합니다.실내 메시 링크와 관련된 모든 경보를 표시합니다.



이러한 경보는 실내 메시 링크에 적용됩니다.

- 불량 링크 SNR - 링크 SNR이 12db 미만이면 이 경보가 생성됩니다.사용자가 이 임계값을 변경할 수 없습니다.하위/상위 항목의 백홀 링크에서 불량 SNR이 탐지되면 트랩이 생성됩니다.트랩에는 SNR 값과 MAC 주소가 포함됩니다.Alarm Severity(경보 심각도)는 Major(주요)입니다.신호 강도가 높아서 수신기 성능을 충분히 보장할 수 없기 때문에 SNR(Signal-to-Noise) 비율이 중요합니다.수신 신호는 존재하는 어떤 소음이나 간섭보다 강력해야 합니다.예를 들어, 강력한 간섭이나 높은 노이즈 수준이 있을 경우 신호 강도가 높고 무선 성능이 저하될 수 있습니다.
- 상위 변경됨 - 하위 항목이 다른 상위 항목으로 이동할 때 이 경보가 생성됩니다.상위 항목이 손실되면 하위 항목이 다른 상위 항목과 조인되며 하위 항목은 이전 상위 주소와 새 상위 MAC 주소를 모두 포함하는 트랩을 WCS에 보냅니다.경보 심각도:정보.
- 자식 이동 - WCS에서 자식 손실 트랩을 가져올 때 이 경보가 생성됩니다.상위 AP에서 하위 AP의 손실을 감지하여 해당 하위 AP와 통신할 수 없으면 하위 손실 트랩을 WCS로 보냅니다.트랩에는 하위 MAC 주소가 포함됩니다.경보 심각도:정보.
- MAP 상위 항목이 자주 변경됨 - 실내 메시 AP가 상위 항목을 자주 변경하는 경우 이 경보가 생성됩니다.MAP 부모 변경 카운터가 지정된 기간 내에 임계값을 초과하면 WCS에 트랩을 보냅니다.트랩에는 MAP 변경 횟수 및 시간 기간이 포함됩니다.예를 들어 2분 내에 5개의 변경 사항이 있을 경우 트랩이 전송됩니다.경보 심각도:정보.
- 1차 하위 구성요소 제외 상위 - 1차 하위 구성요소가 상위 항목을 블랙리스트에 올린 경우 이 경보가 생성됩니다.고정된 시도 횟수 후 하위 항목이 컨트롤러에서 인증하지 못할 경우 하위 항목은 상위 항목을 블랙리스트에 추가할 수 있습니다.자식은 블랙리스트 상위 항목을 기억하며, 자식은 네트워크에 조인할 때 블랙리스트 상위 MAC 주소 및 블랙리스트 기간의 기간이 포함된 트랩을 전송합니다.

실내 메시 링크 이외의 경보:

- 콘솔 포트 액세스 - 콘솔 포트는 고객이 고립된 외부 AP를 복구하기 위해 사용자 이름과 비밀번호를 변경할 수 있는 기능을 제공합니다.그러나 AP에 대한 인증된 사용자 액세스를 방지하려면

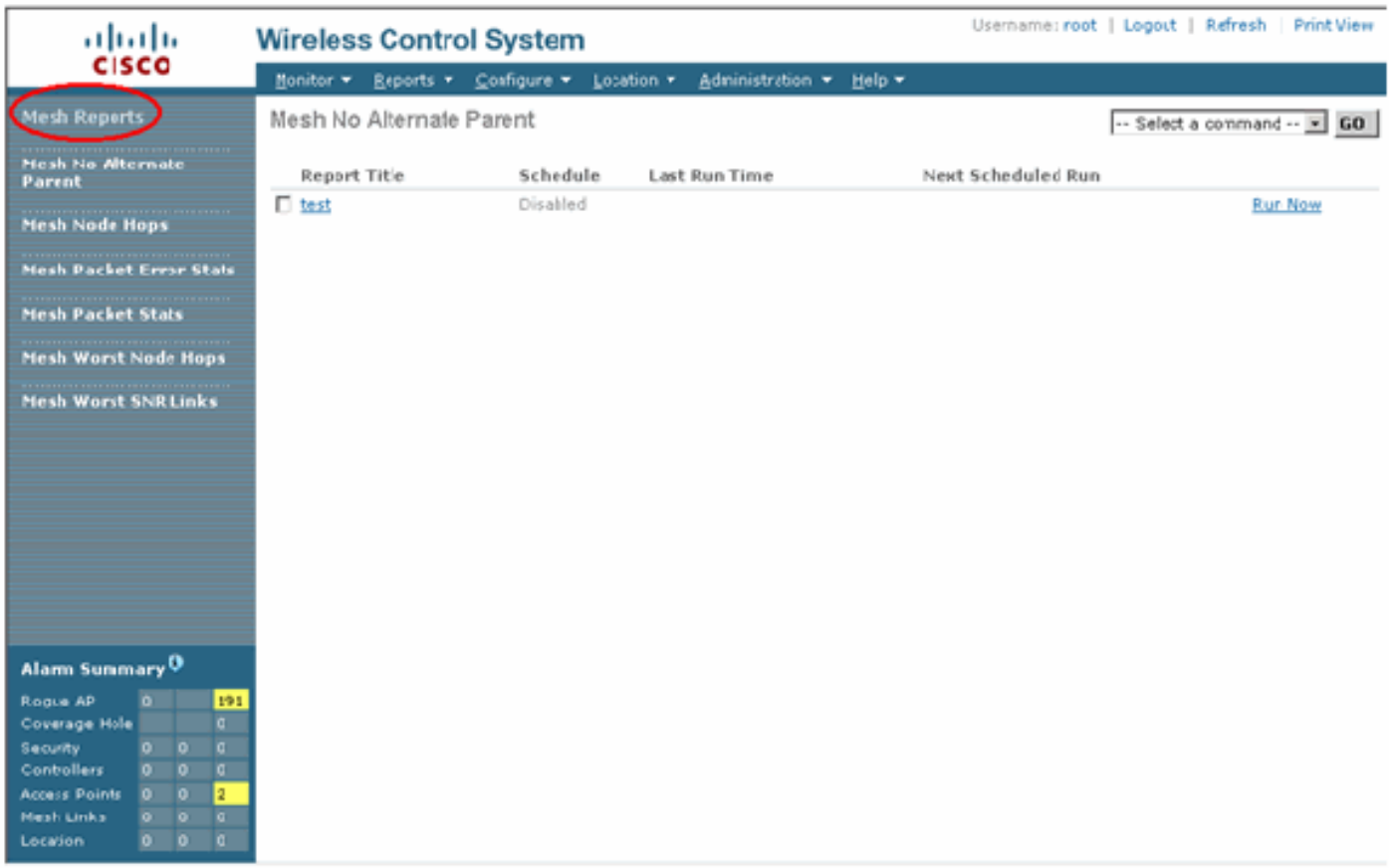
누군가 로그인을 시도할 때 WCS에서 경보를 전송해야 합니다.AP가 실외에 있는 동안 물리적으로 취약하기 때문에 이 알람은 보호를 제공하기 위해 필요합니다.이 경보는 사용자가 AP 콘솔 포트에 성공적으로 로그인했거나 세 번 연속으로 실패한 경우 생성됩니다.

- MAC 권한 부여 실패 - 이 경보는 AP가 실내 메쉬에 참여하려고 하지만 MAC 필터 목록에 없기 때문에 인증하지 못할 때 생성됩니다.WCS는 컨트롤러에서 트랩을 수신합니다.트랩에는 권한 부여에 실패한 AP의 MAC 주소가 포함됩니다.

메시 보고서 및 통계

Cisco는 4.1.185.0에서 향상된 보고서 및 통계 프레임워크를 수행합니다.

- 대체 경로 없음
- 메시 노드 홉스
- 패킷 오류 통계
- 패킷 통계
- Worst Node Hop
- 최악의 SNR 링크



대체 경로 없음

실내 메시 AP는 일반적으로 둘 이상의 인접 디바이스를 가집니다.실내 메시 AP가 상위 링크를 분실하는 경우 AP에서 대체 부모를 찾을 수 있어야 합니다.어떤 경우에는, 만약 이웃이 보이지 않는다면, AP는 그들의 부모를 잃은 경우 다른 부모들에게 갈 수 없을 것입니다.대체 부모가 없는 AP를 사용자가 알아야 합니다.이 보고서에는 현재 상위 이외의 다른 인접 디바이스가 없는 모든 AP가 나열됩니다.

실내 메시 노드 홉스

이 보고서는 루트 AP(RAP)로부터 떨어져 있는 홉의 수를 표시합니다. 다음 기준에 따라 보고서를 생성할 수 있습니다.

- 컨트롤러별 AP
- 층별 AP

패킷 오류율

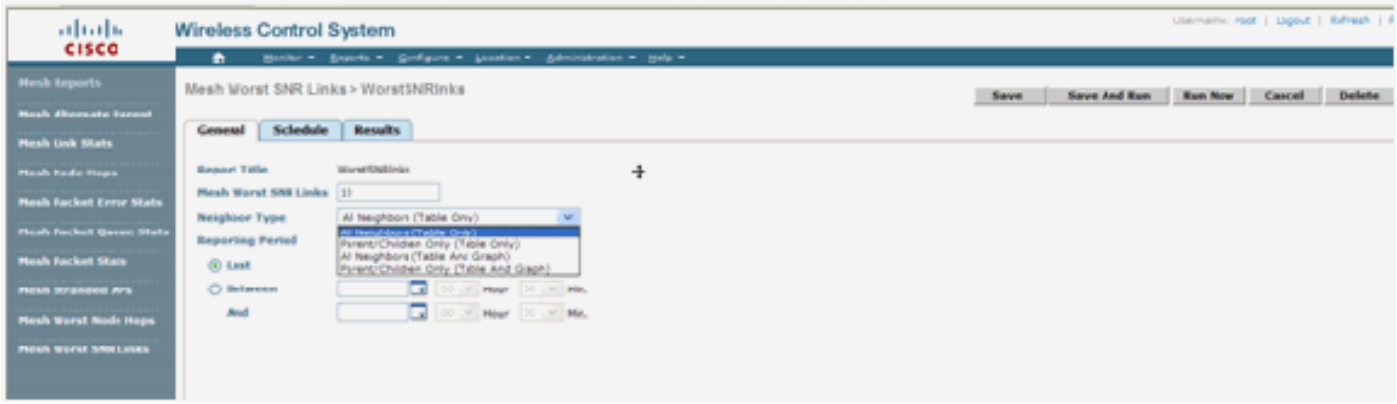
패킷 오류는 간섭 및 패킷 삭제로 인해 발생할 수 있습니다.패킷 오류율 계산은 전송된 패킷 및 성공적으로 전송된 패킷을 기반으로 합니다.패킷 오류율은 백홀 링크에서 측정되며 네이버와 상위 모두에 대해 수집됩니다.AP는 주기적으로 컨트롤러에 패킷 정보를 전송합니다.상위 항목이 변경되면 AP는 수집된 패킷 오류 정보를 컨트롤러에 전송합니다.WCS는 기본적으로 10분마다 컨트롤러에서 패킷 오류 정보를 폴링하고 최대 7일 동안 데이터베이스에 저장합니다.WCS에서 패킷 오류율은 그래프로 표시됩니다.패킷 오류 그래프는 데이터베이스에 저장된 기록 데이터를 기반으로 합니다.

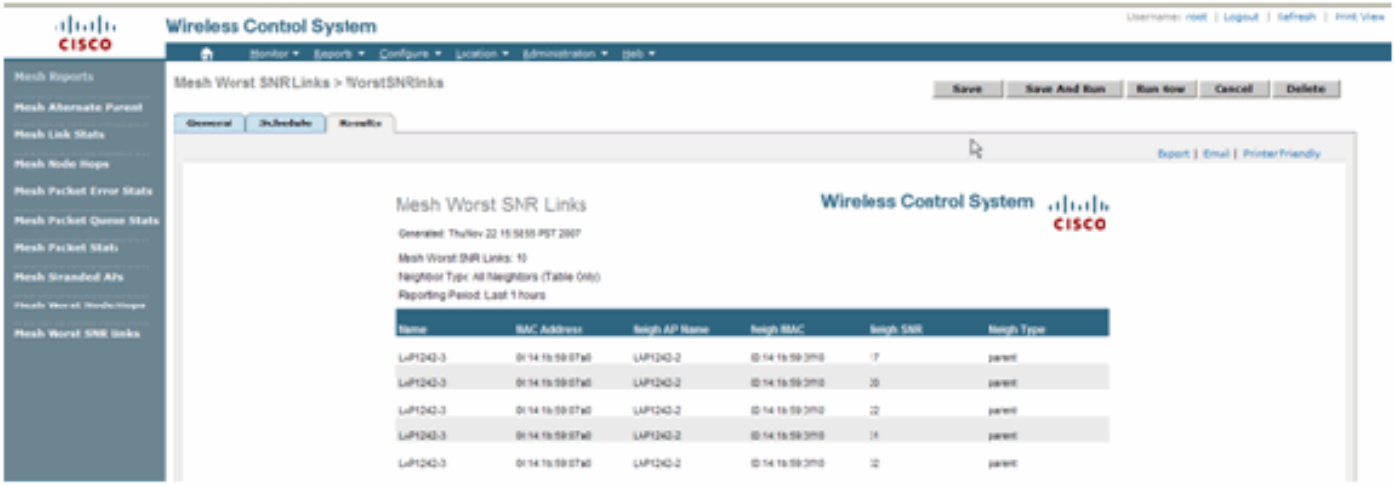
패킷 통계

이 보고서는 네이버 층 전송 패킷 및 성공적으로 전송된 네이버 층 패킷의 카운터 값을 보여줍니다.특정 기준에 따라 보고서를 생성할 수 있습니다.

최악의 SNR 링크

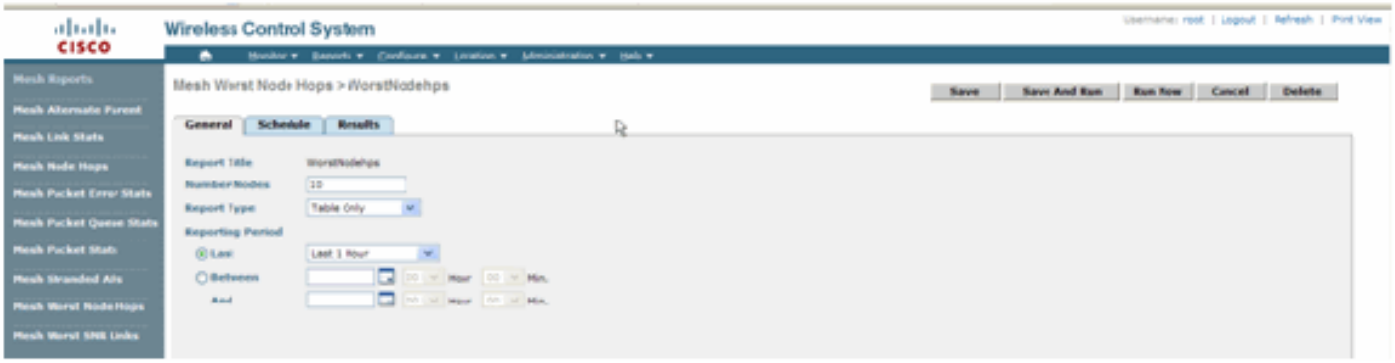
노이즈 문제가 각기 다른 시간에 발생할 수 있으며 노이즈는 다른 속도로 증가하거나 다른 시간 동안 지속될 수 있습니다.다음 그림은 라디오 a 및 b/g와 선택적 인터페이스에 대한 보고서를 생성하는 기능을 제공합니다.보고서에는 기본적으로 최악의 SNR 링크 10개가 나열됩니다.5개 ~ 50개의 최악의 링크를 선택할 수 있습니다.최근 1시간, 최근 6시간, 마지막 날, 마지막 2일, 최대 7일 동안 보고서를 생성할 수 있습니다.데이터는 기본적으로 10분마다 폴링됩니다.데이터는 최대 7일 동안 데이터베이스에 보관됩니다.인접 디바이스 유형 선택 기준은 All Neighbors, Parent/Children일 수 있습니다.



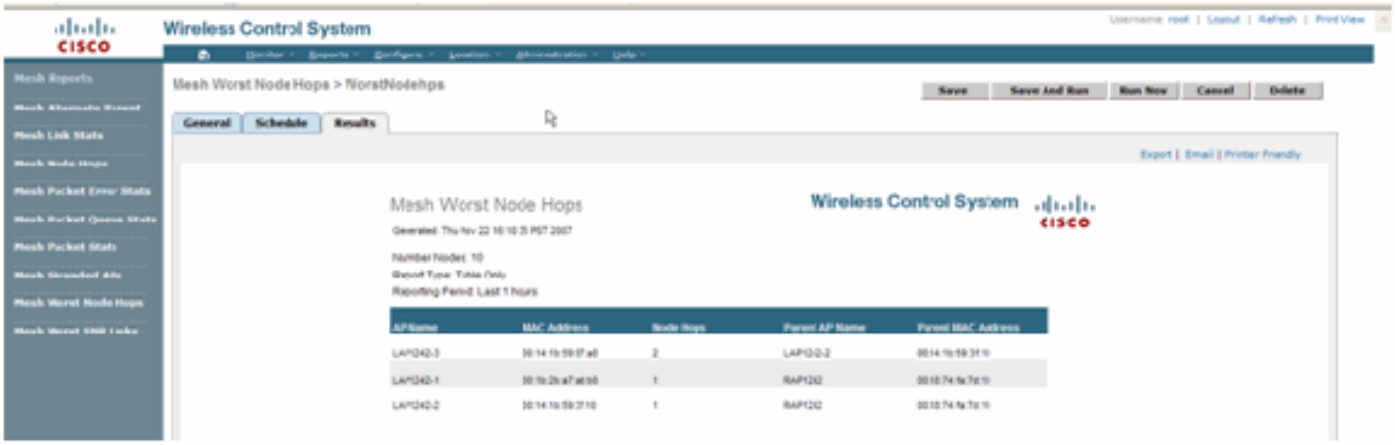


최악의 노드 홉스

이 보고서에는 기본적으로 최악의 홉스 AP가 10개 나열됩니다.AP가 너무 많은 경우 링크가 매우 약할 수 있습니다.사용자는 루트 AP에서 많은 홉이 떨어진 AP를 격리하고 적절한 조치를 취할 수 있습니다.이 **노드 수** 기준을 5에서 50 사이**로** 변경할 수 있습니다. 이 그림의 **보고서 유형** 필터 기준은 테이블만 또는 테이블과 그래프일 수 있습니다.



다음 그림은 마지막 보고서의 결과를 보여줍니다.



보안 통계

실내 메시 보안 통계는 Bridging info(브리징 정보) 섹션의 AP 세부사항 페이지에 표시됩니다.하위 실내 메시 노드가 상위 실내 메시 노드와 연결하거나 인증될 때 실내 메시 노드보안 통계 테이블의 항목이 생성됩니다.실내 메시 노드가 컨트롤러에서 분리되면 항목이 제거됩니다.

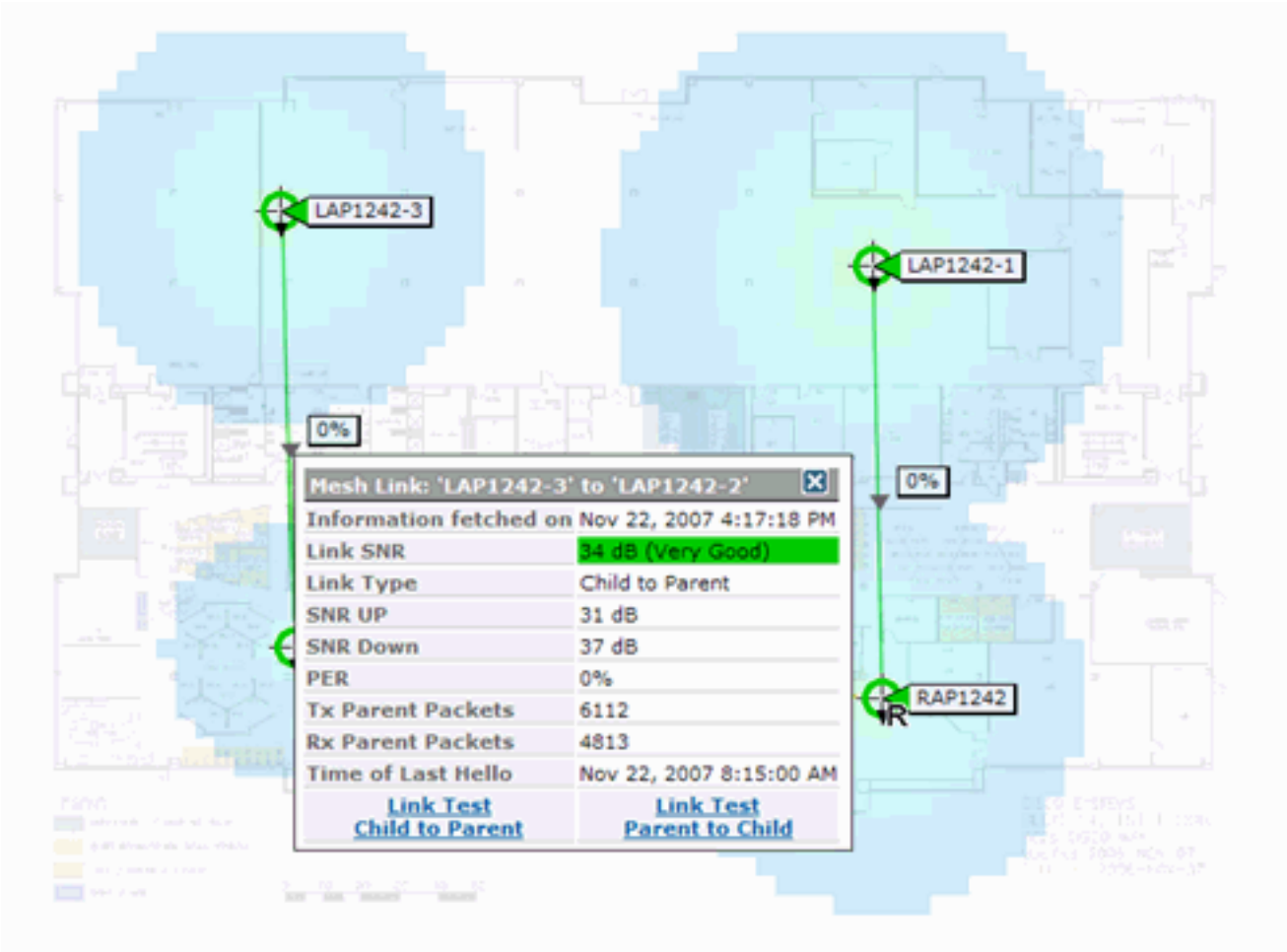
링크 테스트

AP-AP 링크 테스트는 WCS에서 지원됩니다.두 개의 AP를 선택하고 두 AP 간의 링크 테스트를 호출할 수 있습니다.

이러한 AP가 RF 네이버인 경우 링크 테스트에 결과가 발생할 수 있습니다.전체 페이지 새로 고침 없이 맵 자체의 대화 상자에 결과가 표시됩니다.그 대화는 쉽게 처리될 수 있다.

그러나 이러한 2개의 AP가 RF 인접 디바이스가 아닌 경우 WCS는 2개의 AP 간의 경로를 파악하려고 시도하지 않으므로 여러 링크 테스트를 결합합니다.

두 노드 사이의 링크의 화살표 위로 마우스를 이동하면 이 창이 나타납니다.



노드 간 링크 테스트

링크 테스트 툴은 두 AP 간의 링크 품질을 확인하는 온디맨드 툴입니다.WCS에서 이 기능은 AP 세부사항 페이지에 추가됩니다.

AP 세부사항 페이지의 **Indoor Mesh Link** 탭에서 링크 옆에 링크가 나열되면 링크 테스트를 수행할 수 있는 링크가 있습니다.

Controller CLI Link Test 툴에는 선택적 입력 매개 변수가 있습니다.패킷 크기, Total Link 테스트 패킷, 테스트 기간 및 데이터 링크 속도.링크 테스트에는 이러한 선택적 매개변수에 대한 기본값이 있습니다.노드의 MAC 주소만 필수 입력 매개변수입니다.

Link Test 툴은 노드 간에 수신되는 패킷, 전송 강도 등을 테스트합니다.링크 테스트에 대한 링크가

AP 세부 정보 보고서에 표시됩니다.링크를 클릭하면 링크 테스트 결과를 보여 주는 팝업 화면이 나타납니다.링크 테스트는 상위-하위 및 인접 디바이스에만 적용됩니다.

Link Test 출력은 전송된 패킷, 수신된 패킷, 오류 패킷(diff 이유로 버킷), SNR, 노이즈 층 및 RSSI를 생성합니다.

링크 테스트는 최소 GUI에서 다음과 같은 세부 정보를 제공합니다.

- 전송된 링크 테스트 패킷
- 수신된 링크 테스트 패킷
- dBm의 신호 강도
- 신호 대 노이즈 비율

온디맨드 AP 네이버 링크

이는 WCS 맵의 새로운 기능입니다.메시 AP를 클릭하면 세부사항 정보가 있는 팝업 창이 나타납니다.그런 다음 **메시 네이버 보기(View Mesh Neighbors)**를 클릭하면 선택한 AP에 대한 네이버 정보를 가져오고 선택한 실내 메시 AP에 대한 모든 네이버가 있는 테이블이 표시됩니다.

View Mesh Neighbor Link(메시 네이버 보기 링크)에는 강조 표시된 AP의 모든 네이버가 표시됩니다.이 스냅샷은 모든 인접 디바이스, 인접 디바이스 유형 및 SNR 값을 표시합니다.

Ping 테스트

Ping 테스트는 컨트롤러와 AP 간에 ping하는 데 사용되는 온디맨드 툴입니다.Ping 테스트 도구는 AP 세부 정보 페이지와 MAP에서 모두 사용할 수 있습니다.AP 세부사항 페이지 또는 MAP AP 정보에서 **Run Ping Test**(Ping 테스트 실행) 링크를 클릭하여 컨트롤러에서 현재 AP로 ping을 시작합니다.

결론

Enterprise Mesh(즉, 실내 메시)는 유선 이더넷에서 연결을 제공할 수 없는 곳으로 Cisco 무선 커버리지를 확장한 것입니다.엔터프라이즈 메쉬로 무선 네트워크의 유연성과 관리 용이성을 구현할 수 있습니다.

유선 AP가 제공하는 대부분의 기능은 실내 메시 토폴로지에서 제공됩니다.엔터프라이즈 메쉬는 동일한 컨트롤러의 유선 AP와 함께 사용할 수도 있습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems