WLC에 가입하지 못하는 경량 AP 문제 해결

목차

소개

이 문서에서는 WLC(Wireless LAN Controller) 검색 및 가입 프로세스에 대한 개요를 제공합니다.또한 이 문서에서는 LAP(Lightweight Access Point)가 WLC에 조인하지 못하는 이유에 대해 설명하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- LAP 및 Cisco WLC의 컨피그레이션에 대한 기본 지식
- CAPWAP(Lightweight Access Point Protocol)에 대한 기본 지식

표기 규칙

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

WLC(Wireless LAN Controller) 검색 및 가입 프로세스 개요

Cisco Unified Wireless 네트워크에서는 LAP가 먼저 WLC를 검색하고 가입해야 무선 클라이언트에 서비스를 제공할 수 있습니다.

그러나 이는 다음과 같은 질문을 제시합니다.LAP는 다른 서브넷에 있을 때 컨트롤러의 관리 IP 주소를 어떻게 찾았습니까?

컨트롤러가 DHCP 옵션 43을 통해 있는 LAP에 "Cisco-capwap-controller.local_domain"의 DNS 확인 또는 정적으로 구성하지 않으면 LAP는 컨트롤러의 관리 인터페이스를 찾을 네트워크의 위치를 알지 못합니다.

이러한 방법 외에도 LAP는 255.255.255.255 로컬 브로드캐스트가 있는 컨트롤러의 로컬 서브넷을 자동으로 찾습니다.또한 LAP는 재부팅할 때 연결된 컨트롤러의 관리 IP 주소를 기억합니다.따라서 관리 인터페이스의 로컬 서브넷에 LAP를 먼저 넣으면 컨트롤러의 관리 인터페이스를 찾아 주소를 기억하게 됩니다.이를 priming이라고 합니다.나중에 LAP를 교체해도 컨트롤러를 찾을 수 없습니다.따라서 DHCP 옵션 43 또는 DNS 방법을 사용하는 것이 좋습니다.

LAP는 항상 검색 요청을 통해 먼저 컨트롤러의 관리 인터페이스 주소에 연결합니다.그런 다음 컨트롤러는 LAP에 레이어 3 AP 관리자 인터페이스(기본적으로 관리일 수도 있음)IP 주소를 알려 LAP가 다음 AP-manager 인터페이스에 조인 요청을 보낼 수 있도록 합니다.

AP는 시작 시 이 프로세스를 수행합니다.

1. 이전에 고정 IP 주소를 할당하지 않은 경우 LAP가 부팅되고 DHCP가 IP 주소입니다.
2. LAP는 다양한 검색 알고리즘을 통해 컨트롤러에 검색 요청을 보내고 컨트롤러 목록을 작성합니다.기본적으로 LAP는 다음을 통해 컨트롤러 목록의 관리 인터페이스 주소를 최대한 많이 학습합니다.DHCP 옵션 43(지사와 컨트롤러가 다른 대륙에 있는 글로벌 기업에 적합)`cisco-capwap-controller`의 DNS 항목(로컬 비즈니스에 적합 - 새로운 AP가 연결되는 위치를 찾는 데 사용 가능)**참고:** CAPWAP를 사용하는 경우 `cisco-capwap-controller`에 대한 DNS 항목.LAP에서 이전에 기억한 컨트롤러의 관리 IP 주소서브넷의 레이어 3 브로드캐스트정적으로 구성된 정보AP가 마지막으로 조인된 WLC의 모빌리티 그룹에 있는 컨트롤러이 목록에서 구축에 가장 쉽게 사용할 수 있는 방법은 컨트롤러의 관리 인터페이스와 동일한 서브넷에 LAP를 두고 LAPs Layer 3 브로드캐스트가 컨트롤러를 찾도록 허용하는 것입니다.이 방법은 로컬 DNS 서버를 소유하지 않고 소규모 네트워크를 보유한 회사에 사용해야 합니다.다음으로 가장 쉬운 구축 방법은 DHCP와 함께 DNS 항목을 사용하는 것입니다.동일한 DNS 이름의 항목이 여러 개 있을 수 있습니다.이렇게 하면 LAP에서 여러 컨트롤러를 검색할 수 있습니다.이 방법은 모든 컨트롤러가 단일 위치에 있고 로컬 DNS 서버를 소유한 회사에서 사용해야 합니다.또는 여러 DNS 접미사가 있고 컨트롤러가 접미사로 분리되는 경우DHCP 옵션 43은 대기업에서 DHCP를 통해 정보를 현지화하는 데 사용됩니다.이 방법은 단일 DNS 접미사를 가진 대기업에서 사용합니다.예를 들어, Cisco는 유럽, 호주 및 미국에 건물을 소유하고 있습니다.LAPs가 로컬에서 컨트롤러만 조인하도록 하려면 Cisco는 DNS 항목을 사용할 수 없으며 DHCP 옵션 43 정보를 사용하여 LAP에게 로컬 컨트롤러의 관리 IP 주소를 알려 주어야 합니다.마지막으로, 고정 컨피그레이션은 DHCP 서버가 없는 네트워크에 사용됩니다.콘솔 포트 및 APs CLI를

통해 컨트롤러에 조인하는 데 필요한 정보를 정적으로 구성할 수 있습니다.AP CLI를 사용하여 컨트롤러 정보를 정적으로 구성하는 방법에 대한 자세한 내용은 다음 명령을 사용합니다.

```
AP#capwap ap primary-base <WLCName> <WLCIP>
```

DHCP 서버에서 DHCP 옵션 43을 구성하는 방법에 대한 자세한 내용은 DHCP 옵션 43 구성 예를 참조하십시오.

3. 목록의 모든 컨트롤러에 검색 요청을 보내고 시스템 이름, AP-manager IP 주소, 각 AP-관리자 인터페이스에 이미 연결된 AP 수, 컨트롤러의 전체 초과 용량이 포함된 컨트롤러의 검색 응답을 기다립니다.
4. 컨트롤러 목록을 보고 다음 순서로 컨트롤러에 조인 요청을 보냅니다(AP에서 검색 응답을 받은 경우에만).기본 컨트롤러 시스템 이름(이전에 LAP에서 구성됨)보조 컨트롤러 시스템 이름(이전에 LAP에서 구성됨)3차 컨트롤러 시스템 이름(이전에 LAP에서 구성됨)마스터 컨트롤러(LAP가 이전에 기본, 보조 또는 3차 컨트롤러 이름으로 구성되지 않은 경우)어떤 컨트롤러가 새로운 LAP에 가입하는지 항상 아는 데 사용됨)위의 내용이 표시되지 않으면 검색 응답에서 초과 용량 값을 사용하여 컨트롤러 간에 로드 밸런싱을 수행합니다.두 컨트롤러의 용량이 동일한 경우 검색 응답과 함께 검색 요청에 응답한 첫 번째 컨트롤러에 조인 요청을 보냅니다.단일 컨트롤러에 여러 인터페이스에 여러 AP 관리자가 있는 경우 AP 수가 가장 적은 AP-Manager 인터페이스를 선택합니다.컨트롤러는 인증서 또는 AP 자격 증명을 확인하지 않고 모든 검색 요청에 응답합니다.그러나 컨트롤러에서 조인 응답을 받으려면 가입 요청에 유효한 인증서가 있어야 합니다.LAP에서 선택한 조인 응답을 받지 못할 경우 컨트롤러가 구성된 컨트롤러(기본/보조/3차)가 아니면 LAP는 목록에서 다음 컨트롤러를 시도합니다.
5. 가입 회신을 수신하면 AP는 컨트롤러 이미지와 동일한 이미지가 있는지 확인합니다.그렇지 않은 경우 AP는 컨트롤러에서 이미지를 다운로드하고 재부팅하여 새 이미지를 로드하고 1단계에서 프로세스를 다시 시작합니다.
6. 동일한 소프트웨어 이미지가 있는 경우 컨트롤러에서 컨피그레이션을 요청하고 컨트롤러의 등록된 상태로 이동합니다.컨피그레이션을 다운로드한 후 AP가 다시 로드되어 새 컨피그레이션을 적용할 수 있습니다.따라서 추가 다시 로드가 발생할 수 있으며 정상적인 동작입니다.

컨트롤러에서 디버그

컨트롤러에 이 전체 프로세스를 CLI에서 보기 위해 사용할 수 있는 몇 가지 **debug** 명령이 있습니다.

- **디버그 capwap 이벤트 활성화**:검색 패킷 및 조인 패킷을 표시합니다.
- **디버그 capwap 패킷 활성화**:검색 및 조인 패킷의 패킷 레벨 정보를 표시합니다.
- **debug pm pki enable**:인증서 검증 프로세스를 표시합니다.
- **debug disable-all**:디버그를 끕니다.

로그 파일, 콘솔 또는 SSH(Secure Shell)/컨트롤러에 텔넷 출력을 캡처하고 다음 명령을 입력할 수 있는 터미널 애플리케이션을 사용합니다.

```
config session timeout 120
config serial timeout 120
show run-config     (and spacebar thru to collect all)

debug mac addr     (in xx:xx:xx:xx:xx format)
debug client
debug capwap events enable
debug capwap errors enable
debug pm pki enable
```

디버그를 캡처한 후 debug disable-**all** 명령을 사용하여 모든 디버그를 끕니다.

다음 섹션에서는 LAP가 컨트롤러에 등록될 때 이러한 **debug** 명령의 출력을 보여줍니다.

디버그 capwap 이벤트 활성화

이 명령은 CAPWAP 검색 및 가입 프로세스 중에 발생하는 CAPWAP 이벤트 및 오류에 대한 정보를 제공합니다.

다음은 WLC와 동일한 이미지를 가진 LAP에 대한 디버그 capwap **이벤트 enable** 명령 출력입니다.

참고: 공간 제약으로 인해 출력의 일부 행이 두 번째 행으로 이동되었습니다.

```
debug capwap events enable

*spamApTask7: Jun 16 12:37:36.038: 00:62:ec:60:ea:20 Discovery Request from 172.16.17.99:46317
!--- CAPWAP discovery request sent to the WLC by the LAP. *spamApTask7: Jun 16 12:37:36.039:
00:62:ec:60:ea:20 Discovery Response sent to 172.16.17.99 port 46317 !--- WLC responds to the
discovery request from the LAP. *spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join
Request from 172.16.17.99:46317 !--- LAP sends a join request to the WLC.
 *spamApTask7: Jun 16 12:38:33.039: 00:62:ec:60:ea:20 Join Priority Processing status = 0,
Incoming Ap's Priority 1, MaxLrads = 75, joined Aps =0
*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.472: 00:62:ec:60:ea:20 Join Version: = 134256640

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 apType = 46 apModel: AIR-CAP2702I-E-K9

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join resp: CAPWAP Maximum Msg element len =
90

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join Response sent to 172.16.17.99:46317
*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 CAPWAP State: Join
!--- WLC responds with a join reply to the LAP.
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Configuration Status from
172.16.17.99:46317
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 CAPWAP State: Configure !--- LAP requests
for the configuration information from the WLC.

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP info for AP 00:62:ec:60:ea:20 -
- static 0, 172.16.17.99/255.255.254.0, gtw 172.16.16.1
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP 172.16.17.99 ===> 172.16.17.99
for AP 00:62:ec:60:ea:20
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Running spamDecodeVlanProfMapPayload
for00:62:ec:60:ea:20
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Setting MTU to 1485
*spamApTask7: Jun 16 12:38:44.019: 00:62:ec:60:ea:20 Configuration Status Response sent to
172:16:17:99

 !--- WLC responds by providing all the necessary configuration information to the LAP.
*spamApTask7: Jun 16 12:38:46.882: 00:62:ec:60:ea:20 Change State Event Request from
172.16.17.99:46317

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Radio state change for slot: 0 state: 2
cause: 0 detail cause: 69
*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Change State Event Response sent to
172.16.17.99:46317
.
.
.
.
```

```
*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 CAPWAP State: Run

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Sending the remaining config to AP
172.16.17.99:46317!
.
.
.
. !--- LAP is up and ready to service wireless clients. *spamReceiveTask: Jun 16 12:38:46.897:
00:62:ec:60:ea:20 Configuration update request for RrmInterferenceCtrl payload sent to
172:16:17:99

*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for
RrmNeighbourCtrl payload sent to 172.16.17.99

*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for
RrmReceiveCtrl payload sent to 172:16:17:99

*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for
CcxRmMeas payload sent to 172.16.17.99
!--- WLC sends all the RRM and other configuration parameters to the LAP.
```

이전 섹션에서 설명한 것처럼 LAP가 WLC에 등록되면 컨트롤러와 동일한 이미지가 있는지 확인합니다.LAP와 WLC의 이미지가 다른 경우 LAP는 먼저 WLC에서 새 이미지를 다운로드합니다.LAP에 동일한 이미지가 있는 경우 WLC에서 컨피그레이션 및 기타 매개변수를 계속 다운로드합니다.

LAP가 등록 프로세스의 일부로 컨트롤러에서 이미지를 다운로드하는 경우 **debug capwap 이벤트 enable** 명령 출력에서 이러한 메시지를 볼 수 있습니다.

```
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Sending image data block of length 1324 and
msgLength = 1327

*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Image Data Request sent to
172.16.17.201:46318

*spamApTask6: Jun 17 14:23:28.693: 00:62:ec:60:ea:20 Image data Response from
172.16.17.201:46318
```

이미지 다운로드가 완료되면 LAP가 재부팅되어 검색을 실행하고 알고리즘에 다시 연결됩니다.

debug pm pki enable

가입 프로세스의 일부로서 WLC는 인증서가 유효한지 확인하여 각 LAP를 인증합니다.

AP가 WLC에 CAPWAP Join Request를 전송하면 CAPWAP 메시지에 X.509 인증서를 포함합니다.또한 AP는 CAPWAP 가입 요청에도 포함된 임의 세션 ID를 생성합니다.WLC가 CAPWAP Join Request를 수신하면 AP의 공개 키를 사용하여 X.509 인증서의 서명을 확인하고 신뢰할 수 있는 인증 기관에서 인증서를 발급했는지 확인합니다.

또한 AP 인증서의 유효성 간격의 시작 날짜 및 시간을 확인하고 해당 날짜 및 시간을 고유한 날짜 및 시간과 비교합니다(따라서 컨트롤러 시계를 현재 날짜 및 시간과 가깝게 설정해야 함). X.509 인증서가 검증된 경우 WLC는 임의 AES 암호화 키를 생성합니다.WLC는 AES 키를 암호화 엔진으로 배관하여 AP와 교환되는 향후 CAPWAP 제어 메시지를 암호화하고 해독할 수 있습니다.데이터 패킷은 LAP와 컨트롤러 사이의 CAPWAP 터널에서 일반 텍스트로 전송됩니다.

debug **pm pki enable** 명령은 컨트롤러에서 가입 단계 중에 발생하는 인증 검증 프로세스를 표시합니다.AP에 LWAPP **변환** 프로그램에서 생성한 SSC(자체 서명 인증서)가 있는 경우, debug pm pki enable 명령은 조인 프로세스 중에 AP 해시 키도 표시합니다.AP에 MIC(Manufactured Installed Certificate)가 있는 경우 해시 키가 표시되지 않습니다.

참고: 2006년 6월 이후에 제조된 모든 AP에는 MIC가 있습니다.

다음은 MIC가 있는 LAP가 컨트롤러에 조인할 때 **debug pm pki enable** 명령의 출력입니다.

참고: 공간 제약으로 인해 출력의 일부 행이 두 번째 행으로 이동되었습니다.

```
*spamApTask4: Mar 20 11:05:15.687: [SA] OpenSSL Get Issuer Handles: locking ca cert table

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: x509 subject_name
/C=US/ST=California/L=San Jose/O=Cisco Systems/
CN=AP3G2-1005cae83a42/emailAddress=support@cisco.com
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuer_name /O=Cisco
Systems/CN=Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco
Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in
subject is 10:05:ca:e8:3a:42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco
Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in
subject is 10:05:ca:e8:3a:42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Cert Name in subject is
AP3G2-1005cae83a42

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Extracted cert issuer from
subject name.


*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Cert is issued by Cisco
Systems.

*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultMfgCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert
in row 5
*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 260e5e69 for certname cscoDefaultMfgCaCert

*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultMfgCaCert in
row 5 x509 0x2cc7c274

*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName
cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate
<cscoDefaultNewRootCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert
cscoDefaultNewRootCaCert in row 4

*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 28d7044e for certname cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultNewRootCaCert
in row 4 x509 0x2cc7c490
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification return
```

```
code: 1
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification result
text: ok
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert
in row 5

*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: OPENSSL X509_Verify: AP Cert
Verfied Using >cscoDefaultMfgCaCert<

*spamApTask4: Mar 20 11:05:15.691: [SA] OpenSSL Get Issuer Handles: Check cert validity times
(allow expired NO)
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultIdCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching ID cert cscoDefaultIdCert in
row 2
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle: called with 0x1b0b9380

*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle: freeing public key
```

AP에서 디버그

컨트롤러 디버그가 가입 요청을 표시하지 않을 경우 AP에 콘솔 포트가 있는 한 AP에서 프로세스를 디버깅할 수 있습니다. 다음 명령을 사용하여 AP 부팅 프로세스를 볼 수 있지만, 먼저 활성화 모드를 시작해야 합니다(기본 비밀번호는 Cisco입니다).

- **debug dhcp detail**:DHCP 옵션 43 정보를 표시합니다.
- **디버그 ip udp**:AP에서 수신하여 전송된 모든 UDP 패킷을 표시합니다.
- **디버그 capwap 클라이언트 이벤트**:AP에 대한 capwap 이벤트를 표시합니다.
- **디버그 capwap 클라이언트 오류**:AP에 대한 capwap 오류를 표시합니다.
- **dtls 클라이언트 이벤트 디버그**:AP에 대한 DTLS 이벤트를 표시합니다.
- **debug dtls 오류 enable**:AP에 대한 DTLS 오류를 표시합니다.
- **모두 디버그 취소**:AP의 디버그를 비활성화합니다.

다음은 debug capwap 명령의 출력 **예입니다**.이 부분 출력에서는 부팅 프로세스 중에 AP가 컨트롤러를 검색하고 조인하기 위해 전송하는 패킷에 대한 아이디어를 제공합니다.

```
AP can discover the WLC via one of the following options :

!--- AP discovers the WLC via option 43

*Jun 28 08:43:05.839: %CAPWAP-5-DHCP_OPTION_43: Controller address 10.63.84.78 obtained through
DHCP
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.78 with discovery
type set to 2

!--- capwap Discovery Request using the statically configured controller information.

*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.32 with discovery
type set to 1

!--- Capwap Discovery Request sent using subnet broadcast.

*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 255.255.255.255 with
discovery type set to 0
```

```
!--- capwap Join Request sent to AP-Manager interface on DHCP discovered controller.

*Jun 28 08:40:29.031: %CAPWAP-5-SENDJOIN: sending Join Request to 10.63.84.78
```

LAP는 컨트롤러에 조인하지 않습니다. 이유는 무엇입니까?

기본 사항 먼저 확인

- AP와 WLC가 통신할 수 있습니까?
- AP가 DHCP에서 주소를 얻고 있는지 확인합니다(AP의 MAC 주소에 대한 DHCP 서버 임대 확인).
- 컨트롤러에서 AP를 ping해 보십시오.
- VLAN에 대한 패킷이 차단되지 않도록 스위치에서 STP 컨피그레이션이 올바르게 완료되었는지 확인합니다.
- ping이 성공하면 AP에 디버그를 실행하기 위해 단일 WLC 콘솔 또는 텔넷/ssh를 컨트롤러에 검색하는 방법이 하나 이상 있는지 확인합니다.
- AP가 재부팅될 때마다 WLC 검색 시퀀스를 시작하고 AP를 찾으려고 시도합니다.AP를 재부팅하고 WLC에 연결되는지 확인합니다.

다음은 LAP가 WLC에 가입하지 않는 몇 가지 일반적인 문제입니다.

필드 알림:인증서 만료 - FN63942

하드웨어에 포함된 인증서는 제조 후 10년 동안 유효합니다.AP 또는 WLC가 10년 이상 오래된 경우 만료된 인증서로 인해 AP 가입 문제가 발생할 수 있습니다.이 문제에 대한 자세한 내용은 다음 필드 알림을 참조하십시오.

https://www.cisco.com/c/en/us/support/docs/field-notices/639/fn63942.html

고려할 잠재적 문제:예

문제 1:컨트롤러 시간이 인증서 유효성 간격을 벗어납니다.

이 문제를 해결하려면 다음 단계를 완료하십시오.

1. AP에서 **debug dtls 클라이언트 오류 + debug dtls 클라이언트 이벤트** 명령을 실행합니다.

```
*Jun 28 09:21:25.011: DTLS_CLIENT_EVENT: dtls_process_Certificate: Processing...Peer
certificate verification failed 001A
*Jun 28 09:21:25.031: DTLS_CLIENT_ERROR:
../capwap/base_capwap/capwap/base_capwap_wtp_dtls.c:509 Certificate verified failed!
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL : Bad certificate
Alert
```

```
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_client_process_record: Error processing
Certificate.
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_disconnect: Disconnecting DTLS connection
0x8AE7FD0
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_free_connection: Free Called... for
Connection 0x8AE7FD0
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL : Close notify
Alert
```

이 정보는 컨트롤러 시간이 AP의 인증서 유효 간격 외부에 있음을 분명히 보여줍니다.따라서 AP는 컨트롤러에 등록할 수 없습니다.AP에 설치된 인증서에는 사전 정의된 유효성 간격이 있습니다.컨트롤러 시간은 AP 인증서의 인증서 유효성 간격 내에 있는 방식으로 설정해야 합니다.

2. 컨트롤러 CLI에서 **show time** 명령을 실행하여 컨트롤러에서 설정한 날짜와 시간이 이 유효성 간격 내에 있는지 확인합니다.컨트롤러 시간이 이 인증서 유효 간격보다 높거나 낮으면 컨트롤러 시간을 이 간격 내에 포함하도록 변경합니다.**참고:** 컨트롤러에서 시간이 올바르게 설정되지 않은 경우 컨트롤러 GUI 모드에서 **Commands > Set Time**을 선택하거나 컨트롤러 CLI에서 **config time** 명령을 실행하여 컨트롤러 시간을 설정합니다.
3. CLI 액세스 권한이 있는 AP의 경우 AP CLI에서 **show crypto ca certificates** 명령을 사용하여 인증서를 확인합니다.이 명령을 사용하면 AP에 설정된 인증서 유효성 간격을 확인할 수 있습니다.예:

```
AP00c1.649a.be5c#show crypto ca cert
.........................................
.........................................
.........................................
.............................................
Certificate
Status: Available
Certificate Serial Number (hex): 7D1125A900000002A61A
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA SHA2
o=Cisco
Subject:
Name: AP1G2-00c1649abe5c
e=support@cisco.com
cn=AP1G2-00c1649abe5c
o=Cisco Systems
l=San Jose
st=California
c=US
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca2.crl
Validity Date:
start date: 01:05:37 UTC Mar 24 2016
end date: 01:15:37 UTC Mar 24 2026
Associated Trustpoints: Cisco_IOS_M2_MIC_cert
Storage:
...............................
...................................
.....................................
```

이 명령의 출력과 관련된 여러 유효성 간격이 있을 수 있으므로 전체 출력이 나열되지 않습니다.연결된 신뢰 지점에서 지정한 유효성 간격만 고려해야 합니다.이름 필드에 관련 AP 이름이 있는 Cisco_IOS_MIC_cert이 예에서는 `Name`입니다.`C1200-001563e50c7e`.고려할 실제 인증서 유효 간격입니다.

4. CSCuq19142[를 참조하십시오.](#) LAP/WLC MIC 또는 SSC 수명 만료로 DTLS 오류가 발생합니

다.
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCuq19142

문제 2:규정 도메인의 불일치

debug capwap **events enable** 명령 출력에서 다음 메시지가 표시됩니다.

*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configured(BE).
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configured(BE).
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Setting MTU to1485
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: **Country code is not configured(BE).**
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Regulatory Domain Mismatch: AP 00:cc:fc:13:e5:e0 not allowed to join. Allowed domains: 802.11bg:-A
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Finding DTLS connection to delete for AP (192:168:47:29/60390)
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Disconnecting DTLS Capwap-Ctrl session 0x1d4df620 for AP (192:168:47:29/60390). Notify(true)
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 acDtlsPlumbControlPlaneKeys: lrad:192.168.47.29(60390) mwar:10.63.84.78(5246)

WLC msglog will show the following :

```
*spamApTask5: Jun 28 11:52:06.536: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7095
00:cc:fc:13:e5:e0: DTLS connection
closed forAP 192:168:47:28 (60389), Controller: 10:63:84:78 (5246) Regulatory Domain Mismatch
```

이 메시지는 LAP와 WLC의 규정 도메인이 일치하지 않음을 명확하게 나타냅니다.WLC는 여러 규정 도메인을 지원하지만 AP가 해당 도메인에서 가입하려면 각 규정 도메인을 선택해야 합니다.예를 들어 규정 도메인 -A를 사용하는 WLC는 규정 도메인 -A 등을 사용하는 AP에서만 사용할 수 있습니다. AP를 구매할 때 동일한 규정 도메인을 공유하는지 확인합니다.그래야 AP가 WLC에 등록할 수 있습니다.

참고: 802.1b/g 및 802.11a 무선 모두 단일 AP에 대해 동일한 규정 도메인에 있어야 합니다.

문제 3:WLC에서 활성화된 AP 권한 부여 목록권한 부여 목록에 없는 LAP

이러한 경우 debug capwap events enable 명령의 출력에서 컨트롤러에서 이 메시지를 볼 수 있습니다.

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received CAPWAP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 Received CAPWAP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce  00:0B:85:33:52:80
rxNonce  00:0B:85:51:5A:E0
```

```
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 CAPWAP Join-Request MTU path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Wed Sep 12 17:42:50 2007: spamRadiusProcessResponse: AP Authorization failure
for 00:0b:85:51:5a:e0
```

콘솔 포트가 있는 LAP를 사용하는 경우 debug capwap **client error** 명령을 실행하면 다음 메시지가 표시됩니다.

```
AP001d.a245.a2fb#
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: spamHandleJoinTimer: Did not receive the
Join response
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: No more AP manager IP addresses remain.
```

이는 LAP가 컨트롤러의 AP 권한 부여 목록에 속하지 않음을 분명히 나타냅니다.

다음 명령을 사용하여 AP 권한 부여 목록의 상태를 볼 수 있습니다.

```
(Cisco Controller) >show auth-list

Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

AP 권한 부여 목록에 LAP를 추가하려면 **config auth-list add mic *<AP MAC Address>* 명령을** 사용합니다.LAP 권한 부여를 구성하는 방법에 대한 자세한 내용은 Cisco Unified Wireless Network Configuration Example의 LAP(Lightweight Access Point) 권한 부여를 참조하십시오.

문제 4:AP에 인증서 또는 공개 키 손상이 있습니다.

인증서 문제로 인해 LAP가 컨트롤러에 조인하지 않습니다.

debug capwap **오류 enable** 및 debug pm pki enable 명령**을** 실행합니다.손상된 인증서 또는 키를 나타내는 메시지가 표시됩니다.

참고: 공간 제약으로 인해 출력의 일부 행이 두 번째 행으로 이동되었습니다.

```
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 CAPWAP Join Request does not include valid certificate in CERTIFICATE_PAYLOAD
 from AP 00:0f:24:a9:52:e0.
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 Deleting and removing AP 00:0f:24:a9:52:e0 from fast path
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Unable to free public key for AP
```

다음 두 옵션 중 하나를 사용하여 문제를 해결합니다.

- MIC AP - RMA(Return Materials Authorization)를 요청합니다.
- LSC AP - LSC 인증서 다시 프로비저닝

문제 5:컨트롤러가 잘못된 VLAN에서 AP 검색 메시지를 수신합니다(검색 메시지 디버그(응답 없음).

debug capwap **events enable** 명령 출력에서 다음 메시지가 표시됩니다.

Received a Discovery Request with subnet broadcast with wrong AP IP address (A.B.C.D)!

이 메시지는 컨트롤러가 컨트롤러의 구성된 서브넷에 없는 소스 IP 주소가 있는 브로드캐스트 IP 주소를 통해 검색 요청을 받았음을 의미합니다.이는 컨트롤러가 패킷을 삭제하는 것을 의미합니다.

문제는 AP가 검색 요청을 관리 IP 주소로 보내지 않는다는 것입니다.컨트롤러에서 구성되지 않은 VLAN에서 브로드캐스트 검색 요청을 보고하고 있습니다.이 문제는 일반적으로 고객 트렁크가 무선 VLAN으로 VLAN을 제한하는 대신 VLAN을 허용했을 때 발생합니다.

이 문제를 해결하려면 다음 단계를 완료하십시오.

1. 컨트롤러가 다른 서브넷에 있는 경우 AP는 컨트롤러 IP 주소에 대한 준비가 되어야 하며, 그렇지 않으면 AP는 검색 방법 중 하나를 사용하여 컨트롤러 IP 주소를 수신해야 합니다.
2. 이 스위치는 컨트롤러에 없는 일부 VLAN을 허용하도록 구성됩니다.트렁크에서 허용되는 VLAN을 제한합니다.

문제 6:AP가 WLC에 연결할 수 없음, 방화벽 차단 필요 포트

엔터프라이즈 네트워크에서 방화벽을 사용하는 경우 LAP가 컨트롤러에 연결되고 컨트롤러와 통신할 수 있도록 방화벽에서 다음 포트가 활성화되어 있는지 확인합니다.

다음 포트를 활성화해야 합니다.

- CAPWAP 트래픽에 대해 다음 UDP 포트를 활성화합니다.데이터 - 5247제어 - 5246
- 모빌리티 트래픽을 위해 다음 UDP 포트를 활성화합니다.16666년 - 16666년16667년 - 16667년
- CAPWAP 트래픽에 대해 UDP 포트 5246 및 5247을 활성화합니다.
- SNMP용 TCP 161 및 162(WCS[Wireless Control System])

이러한 포트는 선택 사항입니다(요구 사항에 따라 다름).

- TFTP용 UDP 69
- HTTP 또는 HTTPS용 TCP 80 및/또는 443(GUI 액세스용)
- 텔넷용 TCP 23 및/또는 22 또는 CLI 액세스용 SSH

문제 7:네트워크에서 중복 IP 주소

이는 AP가 WLC에 가입하려고 시도할 때 나타나는 또 다른 일반적인 문제입니다.AP가 컨트롤러에 조인하려고 할 때 이 오류 메시지가 표시될 수 있습니다.

No more AP manager IP addresses remain

이 오류 메시지의 이유 중 하나는 AP 관리자 IP 주소와 일치하는 네트워크에 중복 IP 주소가 있을 때 발생합니다.이러한 경우 LAP는 전원 순환을 유지하여 컨트롤러에 연결할 수 없습니다.

디버그에서는 WLC가 AP에서 LWAPP 검색 요청을 수신하고 LWAPP 검색 응답을 AP로 전송함을 보여줍니다.그러나 WLC는 AP로부터 LWAPP 가입 요청을 받지 않습니다.

이 문제를 해결하려면 AP 관리자와 동일한 IP 서브넷의 유선 호스트에서 AP 관리자를 ping합니다

.그런 다음 ARP 캐시를 확인합니다.중복 IP 주소가 있는 경우, 중복 IP 주소가 있는 디바이스를 제거하거나, 네트워크에서 고유한 IP 주소가 있도록 디바이스에서 IP 주소를 변경합니다.

그런 다음 AP가 WLC에 조인할 수 있습니다.

문제 6:메시 이미지가 있는 LAP에서 WLC에 연결할 수 없음

경량 액세스 포인트가 WLC에 등록되지 않습니다.로그에 오류 메시지가 표시됩니다.

```
AAA Authentication Failure for UserName:5475xxx8bf9c User
 Type: WLAN USER
```

이는 경량 액세스 포인트가 메시 이미지와 함께 제공되어 브리지 모드에 있는 경우에 발생할 수 있습니다.LAP가 메시 소프트웨어와 함께 주문된 경우 AP 권한 부여 목록에 LAP를 추가해야 합니다.Security(**보안) > AP Policies(AP 정책**)를 선택하고 **AP**를 Authorization List(권한 부여 목록)에 추가합니다.그런 다음 AP가 가입하고 컨트롤러에서 이미지를 다운로드한 다음 브리지 모드에서 WLC에 등록해야 합니다.그런 다음 AP를 로컬 모드로 변경해야 합니다.LAP는 이미지를 다운로드하고 재부팅한 후 로컬 모드에서 컨트롤러에 다시 등록합니다.

문제 9:주소 "Microsoft DHCP"가 잘못되었습니다.

액세스 포인트는 WLC에 가입하려고 할 때 IP 주소를 매우 빠르게 갱신할 수 있습니다. 이로 인해 Windows DHCP 서버가 이러한 IP를 "BAD_ADDRESS"로 표시하여 DHCP 풀을 신속하게 구축할 수 있습니다.

자세한 내용을 확인하십시오.https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_0101000.html#dhcp-release-override-on-aps