WLC(Wireless LAN Controller) 오류 및 시스템 메시지 FAQ 검토

목차

소개

이 문서에서는 Cisco WLC(Wireless LAN Controller)의 오류 메시지 및 시스템 메시지에 대한 FAQ(자주 묻는 질문)에 대해 설명합니다.

표기 규칙

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

오류 메시지 FAQ

Q. Cisco 4404 WLC를 사용하여 200개 이상의 AP(Access Point)를 Cisco IOS® Software에서 LWAPP(Lightweight AP Protocol)로 변환하기 시작했습니다. 48개 AP의 변환이 완료되었으며 WLC에서 메시지가 수신되었습니다. `[] spam_lrad.c 4212: 1 AP AP .` 오류가 발생한 이유는 무엇입니까?

A. 48개 이상의 AP를 지원하려면 추가 AP-manager 인터페이스를 생성해야 합니다. 그렇지 않으면 다음과 같은 오류가 표시됩니다.

```
Wed Sep 28 12:26:41 2005 [ERROR] spam_lrad.c 4212: AP cannot join because
the maximum number of APs on interface 1 is reached.
```

여러 AP-manager 인터페이스를 구성하고 다른 AP-manager 인터페이스에서 사용하지 않는 기본/백업 포트를 구성합니다. 추가 AP를 표시하려면 두 번째 AP-manager 인터페이스를 생성해야 합니다. 그러나 각 관리자에 대한 기본 포트 및 백업 포트 컨피그레이션이 겹치지 않는지 확인합니다. 즉, AP-manager 1이 포트 1을 기본으로, 포트 2를 백업으로 사용하는 경우 AP-manager 2는 포트 3을 기본으로, 포트 4를 백업으로 사용해야 합니다.

Q. WLC(Wireless LAN Controller) 4402가 있고 1240개의 LAP(Lightweight Access Point)를 사용하고 있습니다. WLC에서 128비트 암호화를 활성화했습니다. WLC에서 128비트 WEP 암호화를 선택하면 1240s에서 128비트가 지원되지 않는다는 오류 메시지가 표시됩니다. `[ERROR] spam_lrad.c 12839: WEP128 CISCO AP xx:xx:xx:xx:xx:xx:xx SSID .` 이 오류가 발생하는 이유는 무엇입니까?

A. WLC에 표시된 키 길이는 실제로 공유 비밀에 있는 비트 수이며 초기화 벡터(IV)의 24비트를 포함하지 않습니다. Aironet 제품을 비롯한 많은 제품에서 128비트 WEP 키라고 합니다. 실제로는 24비트 IV가 있는 104비트 키입니다. 104비트의 키 크기는 128비트 WEP 암호화를 위해 WLC에서 활성화해야 하는 크기입니다.

WLC에서 128비트 키 크기를 선택하면 152비트(128 + 24 IV) WEP 키 암호화가 됩니다. Cisco 1000 Series LAP(AP1010, AP1020, AP1030)만 WLC 128비트 WEP 키 설정을 지원합니다.

Q. 11xx, 12xx 13xx AP 128 WEP ? WLAN . WLC에서 WEP를 구성하려고 하면 오류 메시지가 표시됩니까?

A.무선 LAN 컨트롤러에서 레이어 2 보안 방법으로 고정 WEP를 선택하면 다음 옵션 또는 WEP 키 크기가 있습니다.

- 설정되지 않음
- 40비트
- 104비트
- 128비트

이러한 키 크기 값에는 WEP 키와 연결된 24비트 초기화 벡터(IV)가 포함되지 않습니다. 따라서 64비트 WEP의 경우 WEP 키 크기로 **40**비트를 선택해야 합니다. 컨트롤러는 64비트 WEP 키를 만들기 위해 여기에 24비트 IV를 추가합니다. 마찬가지로 128비트 WEP 키의 경우 **104비트**를 **선택합니다**.

컨트롤러는 152비트 WEP 키(128비트 + 24비트 IV)도 지원합니다. 11xx, 12xx 및 13xx 모델 AP에서는 이 컨피그레이션이 지원되지 않습니다. 따라서 144비트로 WEP를 구성하려고 하면 컨트롤러는 이 WEP 구성이 11xx, 12xx 및 13xx 모델 AP로 푸시되지 않는다는 메시지를 표시합니다.

Q. 클라이언트가 WPA2에 대해 구성된 WLAN에 대해 인증할 수 없으며 컨트롤러가 apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILED: RSN WLAN RSN(WPA2) RSN WARP IE .MobileStation:00:0c:f1:0c:51:22, SSID:<> 오류 메시지. 이 오류가 발생하는 이유는 무엇입니까?

A. 이는 대부분 클라이언트 측의 비호환성 때문에 발생합니다. 이 문제를 해결하려면 다음 단계를 수행하십시오.

- 클라이언트가 WPA2에 대해 Wi-Fi 인증을 받았는지 확인하고 WPA2에 대한 클라이언트 컨피그레이션을 확인합니다.
- 클라이언트 유틸리티가 WPA2를 지원하는지 확인하려면 데이터 시트를 확인하십시오. WPA2를 지원하기 위해 공급업체에서 릴리스한 패치를 설치합니다. Windows 유틸리티를 사용하는 경우 WPA2를 지원하기 위해 Microsoft에서 WPA2 패치를 설치했는지 확인합니다. 자세한 내용은 Microsoft 지원을 참조하십시오.
- 클라이언트 드라이버 및 펌웨어를 업그레이드합니다.
- WLAN에서 Aironet 확장을 끕니다.

Q. WLC를 재부팅하면 7 17 15:23:28 2006 MFP - 3023 Invalid MIC event(s) found as violated with the radio 00:XX:XX:XX:XX and detected by the dot11 interface at slot 0 at AP 00:XX:XX:XX:XX in 300 seconds observing Probe responses, Beacon Frames error message(, 오류 메시지) 표시됩니다. 이 오류는 왜 발생하며 어떻게 제거합니까?

A.이 오류 메시지는 MFP가 활성화된 LAP에서 MIC 값이 잘못된 프레임이 탐지될 때 표시됩니다. MFP에 대한 자세한 내용은 WLC 및 LAP 컨피그레이션 예를 사용한 MFP(Infrastructure Management Frame Protection)를 참조하십시오. 다음 4단계 중 하나를 완료합니다.

1. 네트워크에서 비인가 또는 유효하지 않은 AP 또는 클라이언트를 점검하고 제거하여 유효하지 않은 프레임을 생성합니다.
2. MFP가 활성화되지 않은 그룹의 다른 WLC의 LAP에서 관리 프레임을 들을 수 있으므로 모빌리티 그룹의 다른 구성원에서 MFP가 활성화되지 않은 경우 인프라 MFP를 비활성화합니다. 모빌리티 그룹에 대한 자세한 내용은 WLC(무선 LAN 컨트롤러) 모빌리티 그룹 FAQ를 참조하

십시오.

3. 이 오류 메시지에 대한 수정 사항은 WLC 릴리스 4.2.112.0 및 5.0.148.2에서 확인할 수 있습니다. WLC를 다음 릴리스 중 하나로 업그레이드합니다.
4. 마지막 옵션으로 이 오류 메시지를 생성하는 LAP를 다시 로드해 보십시오.

Q. 클라이언트 AIR-PI21AG-E-K9는 EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)를 통해 액세스 포인트(AP)와 성공적으로 연결되었습니다. 그러나 연결된 AP가 꺼지면 클라이언트는 다른 AP로 로밍하지 않습니다. 이 메시지는 컨트롤러 메시지 로그에 계속 나타납니다. "Fri Jun 2 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922: . . Fri Jun 2 14:48:49 2006 [SECURITY] apf_ms.c 2557: Unable to delete username for mobile 00:40:96:ad:75:f4". 왜 그럴까요?

A.클라이언트 카드가 로밍해야 할 경우 인증 요청을 전송하지만 키를 올바르게 처리하지 않습니다(AP/컨트롤러에 알리지 않고 재인증에 응답하지 않음).

이는 Cisco 버그 IDCSCsd02837에 설명되어 있습니다. 이 버그는 Cisco Aironet 802.11a/b/g 클라이언트 어댑터 설치 마법사 3.5에서 수정되었습니다.

일반적으로, 없음도 다음과 같은 이유로 인해 발생합니다.

- 특정 사용자 이름은 둘 이상의 클라이언트 디바이스에서 사용됩니다.
- 해당 WLAN에 사용되는 인증 방법에 외부 익명 ID가 있습니다. 예를 들어 PEAP-GTC 또는 EAP-FAST에서 일반 사용자 이름을 외부(표시) ID로 정의할 수 있으며, 실제 사용자 이름은 클라이언트와 radius 서버 사이의 TLS 터널 내에 숨겨져 있으므로 컨트롤러가 이를 보고 사용할 수 없습니다. 이러한 경우 이 메시지가 표시될 수 있습니다. 이 문제는 일부 서드파티 및 일부 오래된 펌웨어 클라이언트에서 더 자주 발생합니다.

참고: 등록된 Cisco 사용자만 내부 Cisco 버그 정보 및 툴에 액세스할 수 있습니다.

Q. 6509 스위치에 새 WiSM(Wireless Services Module) 블레이드를 설치하고 Microsoft IAS 서버와 함께 PEAP(Protected Extensible Authentication Protocol)를 구현하는 경우 다음 오류가 표시됩니다. *3 1 00:00:23.526: %LWAPP-5-CHANGED: LWAPP . *3 1 00:00:23.700: %SYS-5-RELOAD: RELOAD requested by LWAPP CLIENT.Reload Reason: FAILED CRYPTO INIT. *3 10:000:000:000:000:00000:00000000000000: %LWAPP-5-CHANGED: LWAPP DOWN *3 1 00:00:23.528: %LWAPP-5-CHANGED: LWAPP DISCOVERY *3 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG:lwapp_crypto_init_ssc_keys_and_certs SSC SSC . *3 1 00:00:23.55: LWAPP_CLIENT_ERROR_DEBUG: *3 10:000:00:23.5.5 7: lwapp_crypto_init: PKI_StartSession *3 1 00:00:23.706: %SYS-5-RELOAD: LWAPP . . 왜 그럴까요?

A.RADIUS 및 dot1x 디버그는 WLC가 액세스 요청을 전송하지만 IAS 서버에서 응답이 없음을 보여줍니다. 문제를 해결하려면 다음 단계를 완료하십시오.

1. IAS 서버 컨피그레이션을 확인하고 확인합니다.
2. 로그 파일을 확인합니다.
3. 인증 세부 정보를 제공할 수 있는 Ethereal과 같은 소프트웨어를 설치합니다.
4. IAS 서비스를 중지하고 시작합니다.

Q. LAP(Lightweight Access Point)는 컨트롤러에 등록하지 않습니다. 무엇이 문제입니까? 컨트롤러에 다음과 같은 오류 메시지가 표시됩니다. Thu Feb 3 03:20:47 2028: LWAPP Join-Request AP 00:0b:85:68:f4:f0 CERTIFICATE_PAYLOAD . Thu Feb 3 03:20:47 2028: AP 00:0B:85:68:F4:F0 .

A. 액세스 포인트(AP)가 LWAPP(Lightweight Access Point Protocol) 가입 요청을 WLC에 전송하면 LWAPP 메시지에 해당 X.509 인증서가 포함됩니다. 또한 LWAPP 가입 요청에 포함된 임의 세션 ID를 생성합니다. WLC가 LWAPP 가입 요청을 수신하면 AP 공개 키로 X.509 인증서의 서명을 검증

하고 해당 인증서가 신뢰할 수 있는 인증 기관에서 발급되었는지 확인합니다. 또한 AP 인증서 유효성 간격의 시작 날짜와 시간을 확인하고 해당 날짜와 시간을 자체 날짜 및 시간과 비교합니다.

이 문제는 WLC의 잘못된 클록 설정 때문에 발생할 수 있습니다. WLC에 시계를 설정하려면 **show time** 및 **config time** 명령을 사용합니다.

Q. LWAPP(Lightweight Access Point Protocol) AP가 컨트롤러에 조인할 수 없습니다. WLC(무선 LAN 컨트롤러) 로그에 다음과 유사한 메시지가 표시됩니다. LWAPP Join-`Request AP 00:0b:85:68:ab:01 CERTIFICATE_PAYLOAD` . 왜 그럴까요?

A.AP와 WLC 간의 LWAPP 터널이 MTU가 1500바이트 미만인 네트워크 경로를 통과하는 경우 이 오류 메시지를 수신할 수 있습니다. 이렇게 하면 LWAPP 패킷이 조각화됩니다. 이것은 컨트롤러에서 알려진 버그입니다. Cisco 버그 IDCSCsd39911을 참조하십시오.

컨트롤러 펌웨어를 4.0(155)으로 업그레이드하는 것이 해결책입니다.

참고: 등록된 Cisco 사용자만 내부 Cisco 버그 정보 및 툴에 액세스할 수 있습니다.

Q. DMZ(De-Militarized Zone)에서 내부 컨트롤러와 가상 앵커 컨트롤러 간에 게스트 터널링을 설정하려고 합니다. 그러나 사용자가 게스트 SSID와 연결하려고 하면 예상대로 DMZ에서 IP 주소를 수신할 수 없습니다. 따라서 사용자 트래픽은 DMZ의 컨트롤러로 터널링되지 않습니다. debug mobile handoff 명령의 출력에는 다음과 유사한 메시지가 표시됩니다. WLAN `<Wlan ID> IP : <controller Ip address>()` . 뭐가 문제죠?

A.게스트 터널링은 기업 무선 네트워크에 대한 게스트 사용자 액세스에 대한 추가 보안을 제공합니다. 이렇게 하면 게스트 사용자가 기업 방화벽을 먼저 통과하지 않고는 기업 네트워크에 액세스할 수 없게 됩니다. 사용자가 게스트 WLAN으로 지정된 WLAN에 연결할 경우 사용자 트래픽은 기업 방화벽 외부의 DMZ에 있는 WLAN 컨트롤러로 터널링됩니다.

이제 이 시나리오를 고려할 때 이 게스트 터널링이 예상대로 작동하지 않는 데에는 몇 가지 이유가 있을 수 있습니다. debugcommand 출력에서 알 수 있듯이, 내부 및 DMZ 컨트롤러의 특정 WLAN에 대해 구성된 보안 정책이 일치하지 않는 것이 문제가 될 수 있습니다. 보안 정책과 다른 설정(예: 세션 시간 초과 설정)이 일치하는지 확인합니다.

이 문제의 또 다른 일반적인 이유는 DMZ 컨트롤러가 특정 WLAN에 대해 자체에 연결되어 있지 않기 때문입니다. 게스트 터널링이 제대로 작동하고 DMZ가 사용자(게스트 WLAN에 속한 사용자)의 IP 주소를 관리하려면 해당 특정 WLAN에 대해 올바른 고정(anchoring)을 수행해야 합니다.

Q. 많은 `"CPU Receive Multicast Queue is full on Controller"` 메시지가 2006 WLC(Wireless LAN Controller)에서 표시되지만 4400 WLC에서는 표시되지 않습니다. 왜 그럴까요? 컨트롤러에서 멀티캐스트를 비활성화했습니다. 2006과 4400 WLC 플랫폼 간의 Multicast Queue Limit의 차이점은 무엇입니까?

A. 컨트롤러에서 멀티캐스트가 비활성화되어 있으므로 이 경보를 발생시키는 메시지는 ARP(Address Resolution Protocol) 메시지일 수 있습니다. 2000 WLC와 4400 WLC 간에는 큐 깊이(512개 패킷)에 차이가 없습니다. 차이점은 4400 NPU가 ARP 패킷을 필터링하는 반면 모든 작업은 2006년에 소프트웨어에서 수행된다는 점입니다. 따라서 2006 WLC에 메시지가 표시되지만 4400 WLC에는 표시되지 않습니다. 44xx WLC는 하드웨어를 통해(CPU를 통해) 멀티캐스트 패킷을 처리합니다. 2000 WLC는 소프트웨어를 통해 멀티캐스트 패킷을 처리합니다. CPU 처리가 소프트웨어보다 더 효율적입니다. 따라서 4400의 대기열은 더 빨리 지워지는 반면 2006 WLC는 이러한 메시지가 많이 표시될 때 약간 어려움을 겪습니다.

Q. "[SECURITY] apf_foreignap.c 763: STA [00:0A:E4:36:1F:9B] Received a packet on port 1 but no Foreignap configured for this port." 내 컨트롤러 중 하나에 오류 메시지가 있습니다. 이 오류는 무엇을 의미하며 이를 해결하기 위해 어떤 단계를 수행해야 합니까?

A.이 메시지는 컨트롤러가 상태 시스템이 없는 MAC 주소에 대한 DHCP 요청을 수신할 때 표시됩니다. 이는 VMWare와 같은 가상 머신을 실행하는 시스템 또는 브리지에서 자주 나타납니다. 컨트롤러는 액세스 포인트(AP)에 연결된 클라이언트와 연결된 주소를 알 수 있도록 DHCP 스누핑을 수행하기 때문에 DHCP 요청을 수신합니다. 무선 클라이언트의 모든 트래픽은 컨트롤러를 통과합니다. 패킷의 대상이 무선 클라이언트인 경우 컨트롤러로 이동한 다음 LWAPP(Lightweight Access Point Protocol) 터널을 지나 AP로 이동한 다음 클라이언트로 꺼집니다. 이 메시지를 완화하기 위해 수행할 수 있는 한 가지 방법은 컨트롤러에서 사용되는 VLAN을 스위치의 **switch port vlan allowcommand**와 함께 컨트롤러로 가는 트렁크에 허용하는 것입니다.

Q. 콘솔에 의 ' ' , ID = 0x0050b986 = 0xfffffffc 오류 메시지가 표시되 ?

A. CPU 로드가 높기 때문일 수 있습니다. 컨트롤러 CPU가 파일 복사 또는 기타 작업을 수행할 때와 같이 로드가 많은 경우, NPU가 컨피그레이션 메시지에 대한 응답으로 전송하는 모든 ACK를 처리할 시간이 없습니다. 이 경우 CPU는 오류 메시지를 생성합니다. 그러나 오류 메시지는 서비스 또는 기능에 영향을 주지 않습니다.

자세한 내용은 Cisco Wireless LAN Controller를 참조하십시오.

Q. WCS(무선 제어 시스템)에서 WEP(Wired Equivalent Privacy) 키 오류 메시지 받았습니다. 스테이션 WEP . MAC 'xx:xx:xx:xx:xx:xx', AP MAC 'xx:xx:xx:xx:xx:xx', ID '1'. 그러나 네트워크에서 보안 매개변수로 WEP를 사용하지 않습니다. Wi-Fi 보호 액세스(WPA)만 사용합니다. 이러한 WEP 오류 메시지가 표시되는 이유는 무엇입니까?

A. 모든 보안 관련 컨피그레이션이 완벽하면 현재 수신하는 메시지는 버그 때문입니다. 컨트롤러에 알려진 몇 가지 버그가 있습니다. "스테이션에 구성된 WEP 키가 **WPA 및 TKIP 클라이언트**와 **각각** 다를 수 있습니다"라고 명시된 Cisco 버그 IDCSCse17260 및 Cisco but ID CSCse11202를 참조하십시오. 실제로 Cisco 버그 ID **CSCse17260**은 Cisco 버그 ID CSCse11202**의 복제본입니다**. Cisco 그러나 ID **CSCse11202**의 수정은 WLC 릴리스 3.2.171.5에서 이미 사용 가능합니다.

> **참고**: 최신 WLC 릴리스에는 이러한 버그에 대한 수정 사항이 있습니다.

> **참고**: 등록된 Cisco 사용자만 내부 Cisco 버그 정보 및 툴에 액세스할 수 있습니다.

Q. 외부 RADIUS 서버를 사용하여 컨트롤러를 통해 무선 클라이언트를 인증합니다. 컨트롤러는 이 오류 메시지를 정기적으로 전송합니다. radius . 이러한 오류 메시지가 표시되는 이유는 무엇입니까?

A. 요청이 WLC에서 RADIUS 서버로 전송되는 경우 각 패킷에는 WLC에서 응답을 기대하는 시퀀스 번호가 있습니다. 응답이 없으면 radius-server not responding을 .

WLC가 RADIUS 서버에서 수신하는 기본 시간은 2초입니다. 이는 WLC GUI의 Security(**보안**) > **authentication-server(인증 서버)에서 설정됩니다**. 최대값은 30초입니다. 따라서 이 문제를 해결하려면 이 시간 초과 값을 최대값으로 설정하는 것이 좋습니다.

RADIUS 서버는 WLC에서 **오는** 요청 패킷의 '무성 폐기'를 수행할 때도 있습니다. RADIUS 서버는 인증서 불일치 및 기타 여러 이유로 인해 이러한 패킷을 거부할 수 있습니다. 이는 서버에서 유효한 작업입니다. 또한 이러한 경우 컨트롤러는 RADIUS 서버가 응답하지 않는 것으로 표시할 수 있습니

다

자동 폐기 문제를 해결하려면 WLC에서 **적극적인** 장애 조치 기능을 비활성화합니다.

WLC에서 **적극적인** 장애 조치 기능이 활성화된 경우, WLC가 너무 적극적이어서 AAA 서버가 응답하지 않는 것으로 표시되지 않습니다. 그러나 AAA 서버는 특정 클라이언트에만 응답할 수 없으므로 이 작업을 수행하지 않아야 합니다(무음 폐기). 유효한 인증서가 있는 다른 유효한 클라이언트에 대한 응답일 수 있습니다. 그러나 WLC는 여전히 AAA 서버가 응답하지 않으며 작동하지 않는 것으로 표시할 수 있습니다.

이 문제를 해결하려면 **적극적인 장애 조치 기능을** 비활성화합니다. 이**를** 수행하기 위해 컨트롤러 **CLI**에서 config radius aggressive-failover disablecommand 명령을 실행합니다. 이 기능이 비활성화되면 RADIUS 서버에서 응답을 받지 못하는 3개의 연속 클라이언트가 있는 경우에만 컨트롤러가 다음 AAA 서버로 장애 조치됩니다.

Q. 여러 클라이언트가 LWAPP에 연결할 수 없으며 컨트롤러가 IAPP-3-MSGTAG015를 기록합니다. `iappSocketTask: iappRecvPkt` 반환했습니다. 왜 이런 일이 일어나죠?

A.이 문제는 CCX v4를 지원하지만 10.5.1.0 이전의 클라이언트 번들 버전을 실행하는 인텔 어댑터의 문제로 인해 주로 발생합니다. 소프트웨어를 10.5.1.0 이상으로 업그레이드할 경우 이 문제가 해결됩니다. 이 오류 메시지에 대한 자세한 내용은 Cisco 버그 IDCSCsi91347을 참조하십시오.

참고: 등록된 Cisco 사용자만 내부 Cisco 버그 정보 및 툴에 액세스할 수 있습니다.

Q. WLC(Wireless LAN Controller)에서 이 오류 메시지가 표시됩니다. `STA 00:05:4e:42:ad:c5 EAP-ID (21)` . 왜 그럴까요?

A.이 오류 메시지는 사용자가 EAP로 보호된 WLAN 네트워크에 연결하려고 시도했으나 미리 구성된 수의 EAP 시도에 실패한 경우 발생합니다. 사용자가 인증에 실패하면 컨트롤러는 클라이언트를 제외하며, 클라이언트는 제외 타이머가 만료되거나 관리자가 수동으로 재정의할 때까지 네트워크에 연결할 수 없습니다.

제외는 단일 디바이스에서 이루어진 인증 시도를 탐지합니다. 해당 디바이스가 최대 실패 횟수를 초과하면 해당 MAC 주소를 더 이상 연결할 수 없습니다.

제외 발생:

- 공유 인증에 대한 5회 연속 인증 실패 후(6차 시도 제외)
- MAC 인증에 대한 5회 연속 연결 실패 후(6차 시도 제외)
- 3회 연속 EAP/802.1X 인증 실패 후(4차 시도는 제외됨)
- 모든 외부 정책 서버 실패(NAC)
- 모든 IP 주소 중복 인스턴스
- 3회 연속 웹 인증 실패 후(4번째 시도 제외)

클라이언트가 제외되는 기간에 대한 타이머를 구성할 수 있으며, 컨트롤러 또는 WLAN 레벨에서 제외를 활성화하거나 비활성화할 수 있습니다.

Q. WLC(Wireless LAN Controller)에서 이 오류 메시지가 표시됨: `1 WLCSCH01/10.0.16.5 . '10.0.16.5'. RADIUS` . 어떤 문제가 있습니까?

A.Cisco 버그 ID CSCsc05495 때문일 수 있습니다. 이 버그 때문에 컨트롤러는 RADIUS RFP를 위반하고 일부 인증 서버에 문제를 일으키는 인증 요청 메시지에 주기적으로 잘못된 AV 쌍(특성 24,

"상태")을 삽입합니다. 이 버그는 3.2.179.6에서 수정되었습니다.

참고: 등록된 Cisco 사용자만 내부 Cisco 버그 정보 및 툴에 액세스할 수 있습니다.

Q. Monitor(모니터) > 802.11b/g Radio(802.11b/g 무선)에서 노이즈 프로파일 오류 메시지가 표시됩니다. 이 FAILED(실패) 메시지가 표시되는 이유를 알고 싶습니다.

A. 노이즈 프로파일 실패/통과 상태는 WLC에서 수행한 테스트 결과 이후에 현재 설정된 임계값과 비교하여 설정됩니다. 기본적으로 노이즈 값은 -70으로 설정됩니다. FAILED 상태는 해당 특정 매개변수 또는 액세스 포인트(AP)의 임계값이 초과되었음을 나타냅니다. 프로필에서 매개변수를 조정할 수 있지만, 네트워크 설계 및 네트워크 성능에 영향을 줄 수 있는 방법을 명확하게 파악한 후 설정을 변경하는 것이 좋습니다.

RRM(Radio Resource Management) PASSED/FAILED 임계값은 **802.11a Global Parameters(802.11a 전역 매개변수) > Auto** RFand **802.11b/g Global Parameters(802.11b/g 전역 매개변수) > Auto** RFpages(자동 RF 페이지)의 모든 AP에 대해 전역적으로 설정됩니다. RRM 통과/실패 임계값은 **802.11** AP Interfaces(**802.11** AP 인터페이스) **> Performance Profile(성능 프로필) 페이지에서** 이 AP에 대해 개별적으로 설정됩니다.

Q. 포트 2를 AP-manager 인터페이스의 백업 포트로 설정할 수 없습니다. 반환된 오류 메시지는 . 관리 인터페이스의 백업 포트로 포트 2를 설정할 수 있습니다. 두 인터페이스의 현재 활성 포트는 포트 1입니다. 왜 그럴까요?

A.AP-Manager에는 백업 포트가 없습니다. 이전 버전에서는 지원되었던 기능입니다. 버전 4.0 이상에서는 AP-manager 인터페이스의 백업 포트가 지원되지 않습니다. 원칙적으로 각 포트에 단일 AP-Manager를 구성해야 합니다(백업 없음). LAG(Link Aggregation)를 사용하는 경우 AP-manager가 하나만 있습니다.

고정(또는 영구) AP-manager 인터페이스는 배포 시스템 포트 1에 할당해야 하며 고유한 IP 주소를 가져야 합니다. 백업 포트에 매핑할 수 없습니다. 일반적으로 관리 인터페이스와 동일한 VLAN 또는 IP 서브넷에 구성되지만 이는 필수 사항이 아닙니다.

Q. 이 오류 메시지가 표시됩니다. `AP '00:0b:85:67:6b:b0'() '00:13:02:8d:f6:41' '1' WPA MIC . 60 .` 왜 그럴까요?

WPA(Wi-Fi Protected Access)에 통합된 MIC(Message Integrity Check)에는 중간자 공격(man-in-the-middle attack)을 방지하는 프레임 카운터가 포함되어 있습니다. 이 오류는 네트워크에 있는 누군가가 원래 클라이언트가 보낸 메시지를 재생하려고 하거나 클라이언트에 오류가 있음을 의미할 수 있습니다.

클라이언트가 MIC 검사에 반복적으로 실패하면 컨트롤러는 60초 동안 오류가 탐지된 AP 인터페이스에서 WLAN을 비활성화합니다. 첫 번째 MIC 실패가 기록되고, 대응책 시행을 가능하게 하기 위해 타이머가 개시된다. 가장 최근의 이전 실패 60초 이내에 후속 MIC 실패가 발생하는 경우, IEEE 802.1X 엔티티가 서플리컨트로서 행동한 STA는 자신을 무효화하거나 IEEE 802.1X 엔티티가 인증자로서 행동한 경우 보안 연계를 가진 모든 STA를 무효화해야 합니다.*

또한 디바이스는 TKIP 암호화 데이터 프레임을 수신 또는 전송하지 않으며, IEEE 802.1X 메시지 이외의 암호화되지 않은 데이터 프레임을 수신 또는 전송하지 않으며, 두 번째 장애를 탐지한 후 최소 60초 동안 어떤 피어와도 송수신하지 않습니다. 디바이스가 AP인 경우 이 60초 기간 동안 TKIP와의 새로운 연결을 허용하지 않습니다. 60초 기간이 끝나면 AP는 정상적인 운영을 재개하고 STA가 (다시) 연결할 수 있도록 합니다.

이렇게 하면 암호화 체계에 대한 가능한 공격을 방지할 수 있습니다. 4.1 이전의 WLC 버전에서는 이러한 MIC 오류를 끌 수 없습니다. Wireless LAN Controller 버전 4.1 이상에서는 MIC 오류에 대한 스캔 시간을 변경하는 명령이 있습니다. 이 명령은 **isconfig wlan security tkip hold-down <0-60초> <wlan id>입니다**. 대책을 위해 MIC 오류 감지를 비활성화하려면 값 0을 사용합니다.

*무효화: 인증을 종료합니다.

Q. 이 오류 메시지는 내 컨트롤러 로그에 표시됩니다. `[ERROR] dhcp_support.c 357: dhcp_bind(): servPort dhcpdate` . 왜 그럴까요?

A.이러한 오류 메시지는 컨트롤러의 서비스 포트에 DHCP가 활성화되어 있지만 DHCP 서버에서 IP 주소를 수신하지 않은 경우 주로 나타납니다.

기본적으로 물리적 서비스 포트 인터페이스에는 DHCP 클라이언트가 설치되어 있으며 DHCP를 통해 주소를 찾습니다. WLC는 서비스 포트에 대한 DHCP 주소를 요청하려고 시도합니다. 사용 가능한 DHCP 서버가 없으면 서비스 포트에 대한 DHCP 요청이 실패합니다. 따라서 오류 메시지가 생성됩니다.

해결 방법은 서비스 포트에 고정 IP 주소를 구성하거나(서비스 포트의 연결이 끊어진 경우에도) DHCP 서버를 사용하여 서비스 포트에 IP 주소를 할당하는 것입니다. 그런 다음 필요한 경우 컨트롤러를 다시 로드합니다.

서비스 포트는 컨트롤러의 OOB(Out of Band) 관리 및 시스템 복구, 네트워크 장애 시 유지 관리를 위해 예약되어 있습니다. 또한 컨트롤러가 부팅 모드에 있을 때 활성화되는 유일한 포트입니다. 서비스 포트는 802.1Q 태그를 포함할 수 없습니다. 따라서 네이버 스위치의 액세스 포트에 연결해야 합니다. 서비스 포트 사용은 선택 사항입니다.

서비스 포트 인터페이스는 서비스 포트를 통한 통신을 제어하며 시스템에 의해 서비스 포트에 정적으로 매핑됩니다. 관리, AP-manager 및 동적 인터페이스와 다른 서브넷의 IP 주소가 있어야 합니다. 또한 백업 포트에 매핑할 수 없습니다. 서비스 포트는 DHCP를 사용하여 IP 주소를 얻거나 고정 IP 주소를 할당할 수 있지만 기본 게이트웨이는 서비스 포트 인터페이스에 할당할 수 없습니다. 고정 경로는 서비스 포트에 대한 원격 네트워크 액세스를 위해 컨트롤러를 통해 정의할 수 있습니다.

Q. 무선 클라이언트가 WLAN(무선 LAN) 네트워크에 연결할 수 없습니다. AP(액세스 포인트)가 연결되어 있는 WiSM은 이 메시지를 보고합니다. `Base Radio MAC 00:0g:23:05:7d:d0, Slot ID 0  Source MAC 00:00:00:00:00:00`. 이것은 무엇을 의미합니까?

A. MAC 계층은 매체에 액세스하기 위한 조건으로 자신의 네트워크 할당 벡터(NAV)의 값을 확인합니다. NAV는 각 스테이션에 상주하는 카운터로서, 이전 프레임이 자신의 프레임을 전송해야 하는 시간을 나타낸다. 스테이션이 프레임을 보내려고 시도하려면 NAV가 0이어야 합니다. 스테이션은 프레임을 전송하기 전에 프레임 길이 및 데이터 전송률을 기반으로 프레임을 전송하는 데 필요한 시간을 계산한다. 스테이션은 이 시간을 나타내는 값을 프레임의 헤더에 있는 지속 시간 필드에 배치합니다. 스테이션이 프레임을 수신하면 이 duration 필드 값을 검토하고 이를 기반으로 해당 NAV를 설정합니다. 이 프로세스에서는 송신 스테이션의 미디어를 예약합니다.

높은 NAV는 팽창된 NAV 값(802.11에 대한 가상 캐리어 감지 메커니즘)의 존재를 나타낸다. 보고된 MAC 주소가 00:00:00:00:00이면 스푸핑된 것일 수 있으며(잠재적으로 실제 공격) 패킷 캡처로 확인해야 합니다.

Q. 컨트롤러를 구성하고 리부팅한 후에는 보안 웹(https) 모드에서 컨트롤러에 액세스할 수 없습니다. 컨트롤러 보안 웹 모드: 보안 웹: 웹 를 찾을 수 () 동안 이 오류 메시지가 . 이 문제의 원인은 무엇입니까?

A. 이 문제와 관련된 몇 가지 이유가 있을 수 있습니다. 하나의 일반적인 이유는 컨트롤러의 가상 인터페이스 컨피그레이션과 관련될 수 있다. 이 문제를 해결하려면 가상 인터페이스를 제거한 다음 다음 다음 명령을 사용하여 다시 생성합니다.

```
WLC>config interface address virtual 1.1.1.1
```

그런 다음 컨트롤러를 재부팅합니다. 컨트롤러가 재부팅되면 다음 명령을 사용하여 컨트롤러에 로컬로 webauth 인증서를 다시 생성합니다.

```
WLC>config certificate generate webauth
```

이 명령의 출력에서 인증서가 생성되었다는 볼 수 .

이제 재부팅 시 컨트롤러의 보안 웹 모드에 액세스할 수 있습니다.

Q. 컨트롤러는 때때로 공격자 MAC 주소가 해당 컨트롤러에 조인된 액세스 포인트(AP)의 주소인 유효한 클라이언트에 대해 이 IDS Disassociation Flood Signature 공격 보고합니다. : IDS 'Disassoc flood' 'x.x.x.x' AP '<AP name>' '802.11b/g' . 'Disassociation flood', 'x'. mac 'hh:hh:hh:hh:hh', 'x', 'x'. 왜 이런 일이 발생할까요?

A.이는 Cisco 버그 IDCSCsg81953 때문입니다.

참고: 등록된 Cisco 사용자만 내부 Cisco 버그 정보 및 툴에 액세스할 수 있습니다.

유효한 클라이언트에 대한 IDS 연결 해제 플러드 공격은 공격자 MAC 주소가 해당 컨트롤러에 조인된 AP의 주소인 경우에 보고되기도 합니다.

클라이언트가 AP에 연결되어 있지만 카드 제거 때문에 통신이 중지되면 AP가 범위를 벗어나서 로밍하는 등 유휴 시간 제한까지 AP가 대기합니다. 유휴 시간 제한에 도달하면 AP가 클라이언트에 연결 해제 프레임을 보냅니다. 클라이언트가 연결 해제 프레임을 승인하지 않으면 AP는 프레임을 여러 번 재전송합니다(약 60프레임). 컨트롤러의 IDS 하위 시스템은 이러한 재전송을 듣고 이 메시지를 통해 알림을 전송합니다.

이 버그는 버전 4.0.217.0에서 해결됩니다. 유효한 클라이언트 및 AP에 대한 이 알림 메시지를 극복하려면 컨트롤러 버전을 이 버전으로 업그레이드하십시오.

Q. 컨트롤러의 syslog에서 [WARNING] apf_80211.c 2408 오류 메시지를 받았습니다. <xx:xx:xx:xx:xx:xx> [ERROR] apf_utils.c 198: . 왜 그럴까요?

A.실제로 Missing Supported Rate(지원 속도 누락) 메시지는 무선 설정에서 특정 필수 데이터 속도에 대해 WLC가 구성되었지만 NIC 카드에 필수 속도가 없음을 나타냅니다.

컨트롤러에서 데이터 속도(예: 1M 및 2M)가 필수 값으로 설정되었지만 NIC 카드가 이러한 데이터 속도로 통신하지 않는 경우 이러한 종류의 메시지를 수신할 수 있습니다. 이는 NIC 카드 오동작입니다. 반면, 컨트롤러가 802.11g로 활성화되어 있고 클라이언트가 802.11b(전용) 카드인 경우 이는 올바른 메시지입니다. 이러한 메시지로 인해 문제가 발생하지 않고 카드가 계속 연결될 수 있는 경우 이러한 메시지는 무시될 수 있습니다. 메시지가 특정 카드인 경우 이 카드의 드라이버가 최신 버전인지 확인합니다.

Q. 이 syslog AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Decode Msg: could not match WLAN ID <id>

오류 메시지가 네트워크에서 브로드캐스트됩니다. 왜 이런 현상이 발생하며 어떻게 중지해야 합니까?

A.이 메시지는 LAP에서 브로드캐스트됩니다. 이는 WLAN에 대한 WLAN 재정의 기능을 구성했으며 특정 WLAN이 알려지지 않은 경우에 나타납니다.

`syslog` 가 있는 경우 특정 IP 주소를 입력하여 중지하거나 특정 IP 주소를 설정할 수 있도록 `ap syslog host global 0.0.0`을 구성합니다.

Q. WLC(무선 LAN 컨트롤러)에서 이 오류 메시지를 받았습니다. `[ERROR] : apf_mm.c : : 581 : Announce collision for mobile 00:90:7a:05:56:8a, .` 왜 그럴까요?

A.일반적으로 이 오류 메시지는 컨트롤러가 무선 클라이언트(즉, 별도의 AP가 클라이언트가 있음을 알린다)에 대해 충돌을 알렸고, 컨트롤러가 한 AP에서 다음 AP로의 핸드오프를 수신하지 않았음을 나타냅니다. 유지 관리할 네트워크 상태가 없습니다. 무선 클라이언트를 삭제하고 클라이언트가 다시 시도하도록 합니다. 이 문제가 자주 발생하면 모빌리티 컨피그레이션에 문제가 발생할 수 있습니다. 그렇지 않으면 특정 클라이언트 또는 상태와 관련된 이상 현상일 수 있습니다.

Q. 내 컨트롤러가 '12' 경보 . 이 오류는 무엇이며 어떻게 해결할 수 있습니까?

A.이 경보 메시지는 클라이언트 SNR(Signal-to-Noise Ratio)이 특정 무선의 SNR 임계값보다 작은 값으로 떨어질 때 발생합니다. 12는 커버리지 홀 감지를 위한 기본 SNR 임계값입니다.

커버리지 홀 검출 및 보정 알고리즘은 클라이언트의 SNR 레벨이 지정된 SNR 임계값보다 작을 때 커버리지 홀이 존재하는지 여부를 결정합니다. 이 SNR 임계값은 AP 전송 전력과 컨트롤러 커버리지 프로파일 값의 두 값에 따라 달라집니다.

구체적으로 클라이언트 SNR 임계값은 각 AP의 전송 전력(dBm으로 표시)에서 상수 값 17dBm을 뺀 값, 사용자 구성 가능한 커버리지 프로필 값을 뺀 값으로 정의됩니다(이 값은 기본적으로 12dB로 설정됨).

- **클라이언트 SNR 차단 값(|dB|) = [AP 전송 전력(dBm) - 상수(17dBm) - 커버리지 프로파일(dB)]**

사용자 구성 가능한 커버리지 프로파일 값은 다음과 같은 방법으로 액세스할 수 있습니다.

1. WLC GUI에서 Wireless(무선)의 주 머리글로 이동하고 왼쪽에서 선택한 WLAN 표준에 대한 **Network(네트워크)** 옵션을 선택합니다(802.11a 또는 802.11b/g). 그런 다음 창 오른쪽 **위**에서 Auto **RF**(자동 RF)를 선택합니다.
2. Auto RF Global parameters(자동 RF 전역 매개변수) 페이지에서 Profile Thresholds(프로파일 임계값) 섹션을 찾습니다. 이 섹션에서는 Coverage (3~50dbm) 값을 찾을 수 있습니다. 이 값은 사용자 구성 가능한 커버리지 프로파일 값입니다.
3. 이 값은 클라이언트 SNR 임계값에 영향을 주도록 편집될 수 있다. 이 SNR 임계값에 영향을 주는 다른 방법은 송신 전력을 증가시키고 커버리지 홀 검출을 보상하는 것이다.

Q. ACS v 4.1 및 4402 WLC(Wireless LAN Controller)를 사용합니다. WLC가 ACS 4.1에 대한 무선 클라이언트의 MAC 인증을 시도할 때 ACS가 ACS에 응답하지 못하고 "*내부 오류가 발생했습니다*"라는 오류 메시지를 보고합니다. 모든 구성이 정확합니다. 이 내부 오류가 발생하는 이유는 무엇입니까?

A.ACS 4.1에 Cisco 버그 IDCSCsh62641과 관련된 인증이 있습니다. 여기서 ACS는 `Internal error has` occurerror 메시지 제공합니다.

이 버그가 문제가 될 수 있습니다. ACS 4.1 다운로드 사이트에 이 버그에 대해 사용 가능한 패치가 있어 문제를 해결할 수 있습니다.

참고: 등록된 Cisco 사용자만 내부 Cisco 버그 정보 및 툴에 액세스할 수 있습니다.

Q. Cisco 4400 Series WLC(Wireless LAN Controller)를 부팅할 수 없습니다. 이 오류 메시지는 컨트롤러에서 수신되었습니다. `** Unable to use ide 0:4 for fatload ** Error (no IRQ) dev 0 blk 0: status 0x51 Error reg: 10 ** Device 0 .` 왜 그럴까요?

A.이 오류의 원인은 하드웨어 문제일 수 있습니다. 이 문제를 더 자세히 해결하려면 TAC 케이스를 여십시오. TAC 케이스를 열려면 Cisco와 유효한 계약을 체결해야 합니다. Cisco TAC에 문의하려면 기술 지원을 참조하십시오.

Q. WLC(Wireless LAN Controller)에서 메모리 버퍼 문제가 발생합니다. 메모리 버퍼가 가득 차면 컨트롤러가 충돌하며 다시 온라인 상태로 전환하려면 컨트롤러를 재부팅해야 합니다. 이러한 오류 메시지는 메시지 로그에 표시됩니다. `Mon 9 10:41:03 2007 [ERROR] dtl_net.c 506: Out of System buffers Mon 9 10:41:03 2007 [ERROR] sysapi_if_net.c 537: Mbuf . 2007 4 9 10:41:03 [ERROR] sysapi_if_net.c 219: MbufGet: no free Mbuf.` 왜 그럴까요?

A.이는 Cisco 버그 IDCSCsh93980 때문입니다. 이 버그는 WLC 버전 4.1.185.0에서 해결되었습니다. 이 메시지를 극복하기 위해 컨트롤러를 이 소프트웨어 버전 이상으로 업그레이드하십시오.

참고: 등록된 Cisco 사용자만 내부 Cisco 버그 정보 및 툴에 액세스할 수 있습니다.

Q. WLC(Wireless LAN Controller) 4400s를 4.1 코드로 업그레이드했는데 syslog에 다음과 같은 메시지가 쏟아졌습니다. `May03 03:55:49.591 dtl_net.c:1191 DTL-1-ARP_POISON_DETECTED: STA [00:17:f2:43:26:93, 0.0.0] ARP (op 1) SPA 192.168.1.233/TPA 192.168.1.233 .` 이 메시지는 무엇을 의미합니까?

A.WLAN이 DHCP required(DHCP 필요)로 표시된 경우 이 오류가 발생할 수 있습니다. 이러한 경우 DHCP를 통해 IP 주소를 수신하는 스테이션만 연결할 수 있습니다. 고정 클라이언트는 이 WLAN에 연결할 수 없습니다. WLC는 DHCP 릴레이 에이전트 역할을 하며 모든 스테이션의 IP 주소를 기록합니다. 이 오류 메시지는 WLC가 스테이션으로부터 DHCP 패킷을 수신하고 IP 주소를 기록하기 전에 WLC가 스테이션으로부터 ARP 요청을 수신할 때 생성됩니다.

Q. Cisco 2106 Wireless LAN Controller에서 PoE(Power over Ethernet)를 사용하는 경우 AP 무선 장치가 활성화되지 않습니다. `AP`에서 . . 오류 메시지가 나타납니다. 이걸 어떻게 고쳐야 하죠?

A.이 오류 메시지는 액세스 포인트의 전원을 켜는 스위치가 예비 표준 스위치이지만 AP가 입력 전원의 예비 표준 모드를 지원하지 않을 때 발생합니다.

Cisco 예비 표준 스위치는 IPM(Intelligent Power Management)을 지원하지 않지만 표준 액세스 포인트에 충분한 전력을 공급하지 않는 스위치입니다.

이 오류 메시지가 표시되는 AP에서 Pre-Standardmode의 전원을 활성화해야 합니다. 이는 컨트롤러 CLI에서 config **ap power pre-standard {enable | disable} {all | Cisco_AP}** 명령.

이전 릴리스에서 소프트웨어 릴리스 4.1로 업그레이드할 경우 필요한 경우 이 명령을 이미 구성해야 합니다. 그러나 새 설치에 대해 이 명령을 입력하거나 AP를 Factory Defaults로 재설정해야 할 수 있습니다.

다음과 같은 Cisco 예비 표준 15W 스위치를 사용할 수 있습니다.

- AIR-WLC2106-K9
- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

Q. 컨트롤러에서 dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED: xx:xx.-xxx.x ARP . . 이와 유사한 syslog 메시지. 이 syslog 메시지는 무엇을 의미합니까?

A. 일부 무선 클라이언트가 ARP 응답을 보내는 동안 NPU(Network Processor Unit)에서 해당 응답을 알아야 합니다. 따라서 ARP 회신은 NPU로 전달되지만 WLC 소프트웨어는 이 항목을 네트워크 프로세서에 추가하려고 시도해서는 안 됩니다. 그러면 이러한 메시지가 생성됩니다. 이로 인해 WLC에 어떤 기능 영향도 없지만 WLC는 이 syslog 메시지를 생성합니다.

Q. 새 Cisco 2106 WLC를 설치하고 구성했습니다. WLC는 온도 센서가 고장 났음을 나타냅니다. "컨트롤러 요약"에서 웹 인터페이스에 로그인하면 내부 온도 옆에 " "라고 표시됩니다. 다른 모든 것은 정상적으로 작동하는 것으로 보입니다.

A. 내부 온도 센서 고장은 외관상이며 WLC 버전 4.2.61.0으로 업그레이드하여 해결할 수 있습니다.

07/01/2007에 구축된 WLC 2106 및 WLC 526은 다른 벤더의 온도 센서 칩을 사용할 수 있습니다. 이 새로운 센서는 잘 작동하지만 4.2 릴리스 이후의 소프트웨어와 호환되지 않습니다. 따라서 이전 소프트웨어는 온도를 읽을 수 없으며 이 오류를 표시합니다. 다른 모든 컨트롤러 기능은 이 결함의 영향을 받지 않습니다.

이 문제와 관련된 알려진 Cisco 버그 IDCSCsk97299가 있습니다. 이 버그는 WLC 버전 4.2의 릴리스 노트에 언급 됩니다.

참고: 등록된 Cisco 사용자만 내부 Cisco 버그 정보 및 툴에 액세스할 수 있습니다.

Q. radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND . WLAN <WLAN ID> RADIUS . . 모든 SSID에 대한 메시지입니다. 이 메시지는 AAA 서버를 사용하지 않는 SSID에 대해서도 나타납니다.

A.이 오류 메시지는 컨트롤러가 기본 RADIUS 서버에 연결할 수 없거나 기본 RADIUS 서버가 정의되지 않았음을 의미합니다.

이 동작의 가능한 원인 중 하나는 버전 4.2에서 해결된 Cisco 버그 IDCSCsk08181입니다. 컨트롤러를 버전 4.2로 업그레이드합니다.

Q. : Jul 10 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL: Interface 1 MAC . WLC(무선 LAN 컨트롤러)에 오류 메시지가 나타납니다. 이것이 무엇을 의미합니까?

A.이는 컨트롤러에서 CPU 소스 패킷을 보내는 동안 오류가 발생했음을 의미합니다.

Q. 이러한 오류 메시지는 WLC(무선 LAN 컨트롤러)에 나타납니다.

- 7 10 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: 'cliWebInitParms.cfg' .
- 7 10 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: 'rfidInitParms.cfg' .

- 7 10 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: 'dhcpParms.cfg' .
- 7 10 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: 'bcastInitParms.cfg' .
- 3 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: . sshpmInitParms.cfg. . - Process: Name:fp_main_task, Id:11ca7618
- 3 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: . bcastInitParms.cfg. . - Process: Name:fp_main_task, Id:11ca7618

Q. 이 오류 메시지가 나타내는 의미는 무엇입니까?

A.이러한 메시지는 정보 메시지이며 일반적인 부팅 절차의 일부입니다. 이러한 메시지는 여러 다른 컨피그레이션 파일을 읽거나 삭제하지 못하여 나타납니다. 특정 컨피그레이션 파일을 찾을 수 없거나 컨피그레이션 파일을 읽을 수 없는 경우 각 프로세스의 컨피그레이션 시퀀스에서 이 메시지를 보냅니다(예: DHCP 서버 컨피그레이션 없음, 태그(RF ID) 컨피그레이션 없음). 이는 무시해도 되는 심각도가 낮은 메시지입니다. 이러한 메시지는 컨트롤러의 작동을 방해하지 않습니다.

Q. **HE6-WLC01,local0,alert,2008-07-25,12:48:18,apf_rogue.c:740 APF-1-UNABLE_TO_KEEP_ROUGE_CONTAINER: Unable to keep ROGUE 00:14:XX:02:XX:XX:XX in contained state - AP** . 오류 메시지가 나타납니다. 이것이 무엇을 의미합니까?

A.이는 비인가 억제 기능을 수행한 AP를 더 이상 사용할 수 없으며, 컨트롤러가 비인가 억제를 수행하는 데 적합한 AP를 찾을 수 없음을 의미합니다.

Q. **DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] SPA 192.168.1.152/TPA 192.168.0.206** 시스템 메시지 **ARP(op 1)** Wireless LAN Controller에 나타납니다. 이 메시지는 무엇을 의미합니까?

A.시스템에서 ARP 스푸핑 또는 중독을 감지했을 수 있습니다. 그러나 이 메시지가 반드시 악성 ARP 스푸핑이 발생했음을 암시하는 것은 아닙니다. 다음 조건이 참일 때 메시지가 나타납니다.

- WLAN은 DHCP Required로 구성되며, 클라이언트 디바이스가 해당 WLAN에 연결된 후 DHCP를 먼저 완료하지 않고 ARP 메시지를 전송합니다. 이는 정상적인 동작일 수 있습니다. 예를 들어 클라이언트가 정적으로 주소가 지정되거나 클라이언트가 이전 연결에서 유효한 DHCP 임대를 보유할 때 발생할 수 있습니다. 오류 메시지는 다음 예제와 같습니다.

```
DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with invalid SPA 192.168.1.152/TPA 192.168.0.206
```

이 조건의 영향은 클라이언트가 WLC를 통해 DHCP를 할 때까지 데이터 트래픽을 보내거나 받을 수 없다는 것입니다.

자세한 내용은 Cisco Wireless LAN Controller 시스템 메시지 가이드의 DTL 메시지 섹션을 참조하십시오.

Q. LAP는 POE(Power over Ethernet)를 사용하여 전원을 켜지 않습니다. Wireless LAN Controller에 대한 로그가 표시됩니다.

AP's Interface:1(802.11a) Operation State Down: Base Radio MAC:XX:1X:XX:AA:VV:CD Cause=Low in-line power

Q. 어떤 문제가 있습니까?

A. POE(Power over Ethernet) 설정이 올바르게 구성되지 않은 경우 이 문제가 발생할 수 있습니다. 경량 모드로 전환된 액세스 포인트(예: AP1131 또는 AP1242 또는 1250 Series 액세스 포인트)가 Cisco pre-IPM(Intelligent Power Management) 스위치에 연결된 파워 인젝터에 의해 전원을 공급받

는 경우 인라인 전원이라고도 하는 PoE(Power over Ethernet)를 구성해야 합니다.

자세한 내용은 PoE(Power over Ethernet), 이더넷 지원 구성을 참조하십시오.

Q. WLC(Wireless LAN Controller)에서 다음 메시지가 표시됩니다.

```
*Mar 05 10:45:21.778: %LWAPP-3-DISC_MAX_AP2: capwap_ac_sm.c:1924 Dropping primary discovery
request from
AP XX:1X:XX:AA:VV:CD - maximum APs joined 6/6
```

Q. Cisco Commerce Workspace

A.Lightweight 액세스 포인트는 컨트롤러를 찾기 위해 특정 알고리즘을 추적합니다. 검색 및 조인 프로세스는 WLC(Wireless LAN Controller)에 LAP(Lightweight AP) 등록에서 자세히 설명합니다.

이 오류 메시지는 WLC에서 최대 AP 용량에 도달한 후 검색 요청을 받으면 표시됩니다.

LAP의 기본 컨트롤러가 구성되지 않았거나 새로운 LAP의 경우 LWAPP 검색 요청을 연결 가능한 모든 컨트롤러에 보냅니다. 검색 요청이 전체 AP 용량으로 실행되는 컨트롤러에 도달하면 WLC는 요청을 가져오고 해당 요청이 최대 AP 용량에 있음을 인식하고 요청에 응답하지 않으며 이 오류를 제공합니다.

Q. LWAPP 시스템 메시지에 대한 자세한 내용은 어디에서 찾을 수 있습니까?

A. LWAPP 시스템 메시지에 대한 자세한 내용은 Cisco Wireless LAN Controller 시스템 메시지 가이드, 4.2(사용 중단됨)를 참조하십시오.

Q. WLC(무선 LAN 컨트롤러)에 Error `extracting webauth files(` 오류) 오류 메시지가 나타납니다. 이것이 무엇을 의미합니까?

번들링된 파일 중 하나라도 파일 이름에 파일 확장명이 포함된 30자를 초과하는 경우 **A.**WLC에서 Custom Web Authentication/Passthrough 번들을 로드하지 못합니다. 사용자 지정 웹 인증 번들에는 파일 이름에 대해 최대 30자로 제한됩니다. 번들 내 파일 이름이 30자를 초과하지 않는지 확인합니다.

Q. 많은 수의 AP 그룹이 포함된 5.2 또는 6.0 코드를 실행하는 WLC(Wireless LAN Controller)에서는 웹 GUI에 구성된 모든 AP 그룹이 표시되지 않습니다. 어떤 문제가 있습니까?

A. CLI를 사용하면 누락된 AP 그룹을 볼 수 있습니다 `show wlan ap-groups`명령을 실행합니다.

목록에 AP 그룹을 하나 더 추가해 보십시오. 예를 들어, 51개의 AP 그룹이 구축되었고 51번째 그룹이 누락되었습니다(3페이지). 52번째 그룹을 추가하면 웹 GUI에 3페이지가 나타나야 합니다.

이 문제를 해결하려면 WLC 버전 7.0.220.0으로 업그레이드하십시오.

관련 정보

- WiSM 문제 해결 FAQ
- 무선 지원 페이지
- Cisco 기술 지원 및 다운로드

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.