

WGB 로밍:내부 세부사항 및 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기규칙](#)

[작업 그룹 브리지란?](#)

[사용 시나리오](#)

[로밍](#)

[로밍 요소](#)

[컨피그레이션 가이드 - 보안 정책](#)

[WPA2-PSK 구성](#)

[802.1x로 WPA2 구성](#)

[CCKM을 사용하여 WPA2 구성](#)

[사용된 메서드의 유효성 검사](#)

[로밍 구성](#)

[패킷 재시도](#)

[RSSI 모니터링](#)

[최소 데이터 전송률](#)

[채널 스캔](#)

[타이머 구성](#)

[기타 WGB 최적화](#)

[무선 관련](#)

[관련 로그](#)

[MFP 사용](#)

[WGB의 EAP-TLS 및 "시계 저장 간격"](#)

[전체 구성 예](#)

[디버그 분석](#)

[관련 정보](#)

소개

Cisco WGB(Workgroup Bridge)는 무선 네트워크를 설계하고 구축하는 데 매우 유용한 툴입니다. 무선 장치가 아닌 장치에서 이동성을 확보할 수 있기 때문입니다.WGB는 사용자의 필요에 따라 구축 시나리오에 영향을 주는 로밍, 보안 액세스 등에 대한 많은 세부 정보를 제공합니다.

코드 버전 12.4(25d)JA 이상에서 Cisco는 고속 로밍 환경에서 WGB 사용을 최적화하기 위해 일련의 명령 및 변경 사항을 도입했습니다.

이 문서에서는 로밍 알고리즘 결정 포인트 및 원하는 사용 모델에 맞게 WGB를 구성하는 방법을 비롯한 WGB의 작동 방식에 대한 다양한 내용을 다룹니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Wireless LAN 솔루션
- Cisco 워크그룹 브리지

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오](#).

작업 그룹 브리지란?

WGB는 기본적으로 인프라에 대한 무선 클라이언트 역할을 하고 이더넷 인터페이스에 연결된 장치에 레이어 2 연결을 제공하도록 구성된 AP(Access Point)입니다.

일반적인 WGB 구축에는 다음과 같은 구성 요소가 있습니다.

- WGB 디바이스, 일반적으로 하나 이상의 라디오 및 이더넷 인터페이스가 있음
- 일반적으로 루트 AP라고 하는 무선 인프라(자동 또는 통합)입니다.
- WGB에 연결된 하나 이상의 유선 클라이언트 장치. 이 문서에서는 혼합 역할 시나리오(WGB로 라디오 하나, 동일한 AP에서 루트로 라디오 하나)에 대해서는 다루지 않습니다.

WGB에는 3가지 주요 유형이 있습니다.

- **Cisco WGB:** Cisco WGB는 WGB(1130, 1240, 1250 등)로 구성된 모든 Cisco IOS® 기반 AP입니다. 이 모드는 IAPP 프로토콜을 사용하여 WGB가 이더넷 인터페이스에서 학습한 디바이스를 네트워크 인프라에 알립니다. 이 경우 WLC(Wireless LAN Controller) 또는 루트 AP는 WGB에서 "연결"된 디바이스에 대한 레이어 2 가시성을 제공합니다.
- **Cisco WGB 이외:** 이 장치는 WGB 역할을 하는 서드파티 디바이스로서 하나 이상의 유선 디바이스를 무선 인프라에 연결합니다. 이들은 IAPP를 지원하지 않으며 단일 유선 장치만 허용하거나 MAC 주소 변환 메커니즘을 제공하여 모든 유선 클라이언트를 단일 802.11 MAC 주소 뒤에 숨깁니다. 이러한 유형의 디바이스는 보안 검사 및 컨트롤러에서 수행한 프레임 처리 때문에 인프라가 WLC인 경우 ARP(Address Resolution Protocol) 및 DHCP 프레임에 대한 특수 처리가 필요합니다.

- "범용 WGB"로 구성된 Cisco AP: 이 모드는 IAPP 메커니즘을 억제하므로 WGB를 Cisco 인프라 또는 서드파티 루트 AP에 사용할 수 있습니다. 이 경우 WGB는 이더넷 클라이언트의 주소를 사용하여 그 뒤에 있는 장치의 수를 1로 제한합니다.

다음 섹션에서는 자동 또는 WLC 인프라에 사용되는 Cisco WGB의 시나리오에 대해 설명합니다.

사용 시나리오

일반적인 WGB의 사용 예는 다음과 같습니다.

- 유선 프린터를 네트워크에 연결
- 다른 제조 구축 - 유선 장치에 케이블을 실행할 수 없거나 실용적이지 않음
- 차량 내 구축 - WGB가 자동차, 지하철, 열차 등의 연결성을 제공하면서 실외 무선 네트워크에 연결
- 유선 카메라

각 예에는 다음 조건에 대한 자체적인 요구 사항이 있습니다.

- 무선 인프라 위에서 실행되는 애플리케이션을 지원하는 데 필요한 대역폭
- 로밍 지연 허용 범위 - 디바이스가 이동하는 동안 WGB가 현재 AP에서 다음 AP로 이동하는 데 얼마나 걸립니까?
- 전달 시간 허용 범위 - 각 로밍에서 손실되는 프레임 수는 몇 개입니까?

프린터가 많이 이동하지 않으므로 로밍 요구 사항이 낮습니다. 반면, 열차는 WGB를 장착하고 있으며, 이동하는 동안 올바른 동작을 보장하려면 로밍 구성 요소를 세밀하게 조정해야 합니다.

비디오 스트림은 대역폭 요구 사항이 클 수 있으므로 무선 데이터 속도가 높습니다. 그러나 텔레메트리 애플리케이션에는 때때로 몇 개의 프레임만 필요할 수 있습니다.

요구 사항은 WGB의 구성뿐만 아니라 무선 인프라를 설계해야 하는 방법에 영향을 주므로 처음부터 올바르게 정의되어야 합니다. 예를 들어, AP 배치, 거리, 전력 레벨, 활성화 속도 등은 모두 로밍 특성에 영향을 미칩니다. 따라서 초고속로밍이 필요한 경우 모든 것이 결정적인 역할을 한다.

일반적으로 다음 세부 사항을 알아야 합니다.

- 애플리케이션에 필요한 대역폭은 얼마입니까?
- 로밍 지연 허용치는 얼마입니까?
- 애플리케이션이 네트워크 연결을 제대로 처리할 수 있습니까? 추가 백업 메커니즘이 있습니까?
- 애플리케이션이 패킷 손실을 제대로 처리할 수 있습니까?(최상의 무선 설계에서도 패킷 손실이 예상되어야 합니다.)

이 문서에서는 고속 로밍/실외 RF 환경을 설계하는 방법에 대한 자세한 내용은 다루지 않습니다. 실외 메시 구축 가이드를 참조하십시오.

로밍

무선 장치의 경우 로밍은 기능의 매우 중요한 부분입니다.

기본적으로 로밍은 동일한 무선 인프라에 속하는 한 AP에서 다른 AP로 이동하는 기능을 의미합니다.

로밍은 현재 AP에서 다음 AP로의 변경이 필요하므로, 서비스 없는 연결 해제 또는 시간이 발생합니다.

다.이 연결 끊기는 작은 것일 수 있습니다.예를 들어, 보안이 필요한 경우 음성 구축에서 200ms 미만 또는 훨씬 더 오래, 심지어 초 단위까지 각 로밍 이벤트에 전체 인증을 적용할 수 있습니다.

로밍이 필요합니다. 그러면 디바이스가 희망적으로 더 나은 신호를 가진 새 부모를 찾을 수 있고 네트워크 인프라에 계속 제대로 액세스할 수 있습니다.동시에 너무 많은 로밍으로 인해 여러 개의 연결이 끊어지거나 서비스가 없는 시간이 발생할 수 있으며 이는 액세스에 영향을 줍니다.WGB와 같은 모바일 디바이스에서는 다양한 RF 환경 및 데이터 요구 사항에 적응할 수 있는 충분한 컨피그레이션 기능을 갖춘 우수한 로밍 알고리즘을 갖추는 것이 중요합니다.

로밍 요소

- **트리거:**각 클라이언트 구현에는 하나 이상의 트리거 또는 이벤트가 있으며, 이 이벤트가 충족되면 디바이스가 다른 상위 AP로 이동하게 됩니다.예:비컨 손실(디바이스는 AP에서 더 이상 일한 신호를 수신하지 않음), 패킷 재시도, 신호 레벨, 수신된 데이터 없음, 수신된 디인증 프레임, 사용 중인 데이터 속도 감소 등 가능한 트리거는 완전히 표준화되지 않으므로 클라이언트 구현과 다를 수 있습니다.더 간단한 장치에는 트리거 세트가 불량하여(스티커 클라이언트) 또는 불필요한 로밍이 발생할 수 있습니다.WGB는 이전에 설명한 모든 이전 요소를 지원합니다.
- **스캔 시간:**무선 장치(WGB)는 잠재적 부모를 검색하는 데 약간의 시간을 소비합니다.이는 일반적으로 서로 다른 채널에서 AP를 능동적으로 탐색하거나 수동적으로 수신하는 것을 의미합니다.무선이 스캔해야 하므로 WGB가 데이터 포워딩과 다른 작업을 수행하는 데 걸리는 시간을 의미합니다.이 스캔 시간부터 WGB는 로밍할 수 있는 유효한 부모 집합을 만들 수 있습니다.
- **상위 선택:**스캔 시간 후 WGB는 잠재적 상위 항목을 확인하고, 가장 적합한 상위 항목을 선택하고, 연결/인증 프로세스를 트리거할 수 있습니다.로밍 이벤트에서 큰 이점이 없을 경우(로밍을 너무 많이 수행하면 안 될 수 있음), 의사 결정 지점은 현재 부모에 남아 있을 수 있습니다.
- **연결/인증:**WGB는 일반적으로 802.11 인증 및 연결 단계를 모두 포함하는 새 AP에 연결되며 SSID(WPA 2-PSK, CCKM, 없음 등)에 구성된 보안 정책을 완료합니다.
- **트래픽 전달 복원:**WGB는 로밍 후 IAPP 업데이트를 통해 알려진 유선 클라이언트의 네트워크 인프라를 업데이트합니다.이 시점 이후에는 유선 클라이언트와 네트워크로 가는 트래픽이 다시 시작됩니다.

컨피그레이션 가이드 - 보안 정책

모바일 장치에서 로밍하는 데 중요한 요소 중 하나는 인프라에 구현할 보안 정책입니다.여러 가지 옵션이 있으며, 각 옵션에는 좋은 점/나쁜 점이 있습니다.가장 중요한 것은 다음과 같습니다.

- **개방성** - 기본적으로 보안이 없습니다.이는 모든 정책에서 가장 빠르고 간단합니다.이는 인프라에 대한 무단 액세스를 제한하지 않고 공격에 대한 보호를 수행하지 않는 주된 문제를 갖고 있으며, 이는 해당 사용을 매우 구체적인 시나리오로 제한합니다.예를 들어 구축의 단순한 특성으로 인해 외부 공격이 불가능한 지위를 예로 들 수 있습니다.
- **MAC 주소 인증** - 기본적으로 MAC 주소 스푸핑은 간단한 공격이므로 개방과 동일한 수준의 보안을 제공합니다.MAC 검증을 완료하는 데 시간이 추가되어 로밍 속도가 느려지기 때문에 권장되지 않습니다.
- **WPA2-PSK - AES-CCMP(Good Level Encryption)**를 제공하지만 인증 보안은 사전 공유 키의 품질에 따라 달라집니다.보안 측정의 경우 12자 이상의 비밀번호와 임의의 비밀번호를 사용하는 것이 좋습니다.사전 공유 키 방법과 마찬가지로, 키가 여러 디바이스에서 사용되므로, 키가 손상된 경우 모든 장비에서 비밀번호를 수정해야 합니다.로밍 속도는 6개의 프레임 교환에서 수행되므로 허용되며, 외부 장비(RADIUS 서버 없음 등)를 포함하지 않으므로 완료될 때 최대/하위 시간 범위를 계산할 수 있습니다.일반적으로 이 방법은 문제와 이점을 균형 있게 정리한

후에 선호되는 방법입니다.

- **802.1x를 사용하는 WPA2**—장치/사용자 자격 증명별로 개별적으로 변경할 수 있는 이전 방법을 사용하여 이전 방법을 개선합니다.가장 큰 문제는 로밍의 경우 디바이스가 빠르게 이동하거나 짧은 로밍 시간이 필요할 때 이 방법이 제대로 작동하지 않는다는 것입니다.일반적으로 이 옵션은 동일한 6 프레임 + 4~의 EAP 교환을 사용합니다.이는 선택한 EAP 유형과 인증서 크기에 따라 달라집니다.일반적으로 이 작업은 10~20개의 프레임과 더불어 RADIUS 서버 처리의 추가 지연이 필요합니다.
- **WPA2+CCKM**—이 메커니즘은 보호 기능을 제공하며 802.1x를 사용하여 초기 인증을 구축한 다음 각 로밍 이벤트에서 2프레임만 빠르게 교환합니다.로밍 시간이 매우 빠릅니다.주요 문제는 로밍이 실패하면 802.1x로 되돌아갑니다.그런 다음 인증 후 CCKM 사용을 다시 시작합니다.WGB 위에 있는 애플리케이션이 문제가 발생할 경우 비정기적으로 로밍 시간을 허용할 수 있는 경우 PSK에 비해 최상의 옵션으로 사용할 수 있습니다.

이 문서에서는 LEAP, WPA-TKIP, WEP 등과 같은 보안 문제가 있는 권장되지 않는 기술을 다루지 않습니다.

[WPA2-PSK 구성](#)

WGB에서는 구성이 매우 간단합니다.SSID 정의 및 무선 장치에 적절한 암호화가 필요합니다.

```
dot11 ssid wgbpsk
vlan 32
authentication open
authentication key-management wpa version 2
wpa-psk ascii YourReallySecurePSK!
no ids mfp client
```

```
interface Dot11Radio0
ssid wgbpsk
encryption mode ciphers aes-ccm
station-role workgroup-bridge
```

SSID 이름과 사전 공유 키는 네트워크 인프라와 일치해야 합니다.

[802.1x로 WPA2 구성](#)

기본적으로 이전 컨피그레이션의 위에 구축되며 EAP 프로파일 및 인증 방법이 추가됩니다.

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management wpa version 2
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
eap profile eapfast
!--- This covers the EAP method type used on your network. method fast ! ! dot1x credentials wgb
!--- This is your WGB username/password. username cisco password 7 1511021F0725 interface
Dot11Radio0 encryption mode ciphers aes-ccm ssid wlan1
```

[CCKM을 사용하여 WPA2 구성](#)

WPA2에서 단 하나의 사소한 변경 사항이 있는 한 단계만 사용할 수 있습니다.SSID 컨피그레이션

에서 CCKM 플래그를 사용합니다.이렇게 하면 WLAN이 WLC 측에서만 CCKM에 대해 구성된 것으로 가정합니다.

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management cckm
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
```

사용된 메서드의 유효성 검사

WGB를 빠르게 검사하면 CCKM에서 사용 중인 암호화 및 키 관리를 보고할 수 있습니다.

```
wgb-1260#sh dot11 associations a1
Address          : 0024.97f2.75a0      Name           : lap1140-etsi-1
IP Address       : 192.168.40.10      Interface      : Dot11Radio 0
Device           : LWAPP-Parent       Software Version : NONE
CCX Version      : 5                  Client MFP     : Off

State            : EAP-Assoc          Parent         : -
SSID             : wlan1
VLAN             : 0
Hops to Infra   : 0                  Association Id  : 1
Tunnel Address   : 0.0.0.0
Key Mgmt type   : CCKM              Encryption    : AES-CCMP

Current Rate     : m7.-              Capability     : WMM ShortHdr ShortSlot
Supported Rates  : 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7.
Voice Rates      : disabled           Bandwidth     : 20 MHz
Signal Strength  : -59 dBm            Connected for  : 72 seconds
Signal to Noise  : 41 dB              Activity Timeout : 8 seconds
Power-save       : Off                Last Activity   : 7 seconds ago
Apsd DE AC(s)   : NONE

Packets Input    : 12064              Packets Output : 136
Bytes Input      : 2892798            Bytes Output   : 19514
Duplicates Rcvd  : 87                 Data Retries   : 8
Decrypt Failed   : 0                  RTS Retries    : 0
MIC Failed       : 0                  MIC Missing    : 0
Packets Redirected: 0                 Redirect Filtered: 0
```

로밍 구성

WGB에서 로밍 알고리즘에 영향을 주는 여러 매개변수를 수정할 수 있습니다.

패킷 재시도

기본적으로 WGB는 프레임을 64번 재전송합니다.상위 항목에서 (ACK) 를 올바르게 승인하지 않으면 상위 항목이 더 이상 유효하지 않은 것으로 간주하여 스캔/로밍 프로세스를 시작합니다.이 트리거를 "async" 로밍 트리거로 봅니다. 전송이 실패할 때마다 수행할 수 있기 때문입니다.

이를 구성하는 명령은 dot11 인터페이스 안으로 이동하고 다음 옵션을 사용합니다.

packet retries NUM [drop]

번호:기본값은 1~128이며 기본값은 64입니다. 빠른 로밍 트리거의 올바른 숫자는 일반적으로 32입니다. 낮은 숫자를 사용하는 것은 대부분의 RF 환경에서 권장되지 않습니다.

삭제:WGB가 없으면 최대 재시도에 도달할 때 로밍 이벤트가 시작됩니다.WGB는 새 로밍을 시작하지 않으며 신호 손실 및 신호 등 다른 트리거를 사용합니다.

RSSI 모니터링

WGB는 현재 상위에 대해 사전 활성 신호 스캔을 구현하고 신호가 예상 수준 아래로 떨어지면 새 로밍 프로세스를 시작할 수 있습니다.

이 프로세스에서는 두 가지 매개 변수를 사용합니다.

- X초마다 확인 프로세스를 깨우는 타이머
- RSSI 레벨 - 현재 신호가 낮을 경우 로밍 프로세스를 시작하는 데 사용됩니다.

예를 들면 다음과 같습니다.

in d0

mobile station period 4 threshold 75

일부 조건에서 "로밍 루프"를 방지하거나 너무 적극적인 로밍 동작을 피하기 위해 인증 프로세스를 완료하는 데 WGB가 걸리는 시간이 이보다 짧으면 안 됩니다.일반적으로 애플리케이션의 요구 사항을 충족하는지 테스트해야 합니다.

PSK의 경우 EAP 기반 방식보다 낮을 수 있습니다(매우 포괄적인 애플리케이션의 경우 일반 2 및 4).

RSSI 레벨은 기본적으로 일반 -dBm 측정 레벨이지만 양의 정수로 표현됩니다.데이터 속도가 제대로 작동하도록 하는 데 필요한 최소값보다 약간 높은 숫자를 사용해야 합니다.예를 들어, 원하는 최소 속도가 6mbps이면 임계값 RSSI가 -87이면 충분합니다.48mbps의 경우 -70dBm 등이 필요합니다.

참고: 이 명령은 너무 포괄적인 "데이터 속도 변경에 따른 로밍"을 트리거할 수도 있습니다.좋은 결과를 얻으려면 최소값과 함께 사용해야 합니다.

최소 데이터 전송률

12.4(25d)JA부터 Cisco는 WGB가 새 로밍 이벤트를 트리거해야 하는 시기를 제어할 수 있는 구성 가능한 매개변수를 추가했습니다. 이 경우 상위 데이터에 대한 현재 데이터 속도가 지정된 값보다 낮습니다.

따라서 비디오 또는 음성 애플리케이션을 지원하기 위해 원하는 낮은 속도의 속도를 유지할 수 있습니다.

이 명령을 사용할 수 있기 전에 속도가 이전 시간보다 낮은 것으로 확인되었을 때 WGB가 로밍을 자주 트리거했습니다.기본적으로 X+1에 맞춰서 속도가 이전 X 시간보다 낮으면 WGB가 로밍 프로세스를 시작했습니다.로그에 다음 메시지가 표시됩니다.

```
*Mar 1 00:36:43.490: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio1, parent lost: Had to lower data rate
```

이는 너무 포괄적이며 일반적으로 유일한 솔루션은 WGB 및 상위 AP에서 단일 데이터 전송률을 구성하는 것이었습니다.

이제 모바일 스테이션 period 명령을 사용할 때마다 이 명령을 항상 구성하는 것이 좋습니다.

```
in d0
mobile station minimum-rate 2.0
```

이렇게 하면 현재 속도가 구성된 값보다 낮은 경우에만 새 로밍 프로세스가 트리거됩니다. 따라서 불필요한 로밍이 줄어들고 예상 속도 값을 유지할 수 있습니다.

참고: "Had to lower data rate" 메시지는 이 컨피그레이션에서도 발생할 것으로 예상되며, WGB가 구성된 속도보다 낮은 TX인 경우 모바일 스테이션 기간 확인 시간이 트리거된 경우에만 표시됩니다.

채널 스캔

WGB는 로밍 이벤트를 수행하는 동안 모든 "국가 채널"을 스캔합니다. 즉, 무선 도메인에 따라 2.4GHz 대역에서 채널 1~11을 스캔하거나 1~13을 스캔할 수 있습니다.

스캔한 채널마다 시간이 걸립니다. 802.11bg는 약 10~13ms입니다. 802.11a에서 채널이 DFS를 사용하는 경우 최대 150ms가 될 수 있습니다(프로브는 하지 않고 수동 스캔만 수행).

적합한 최적화는 스캐닝된 채널이 인프라에서 사용 중인 채널만 사용하도록 제한하는 것입니다. 채널 목록이 커서 802.11a에서 특히 중요합니다. DFS를 사용하는 경우 채널당 시간이 길어질 수 있습니다.

WGB/로밍용 채널 계획을 설계할 때는 다음 세 가지 사항을 고려해야 합니다.

- 2.4GHz 대역의 경우 1/6/11을 고수하여 측면 채널 간섭을 최소화하십시오. 4개 등이 포함된 다른 모든 채널 계획은 RF의 관점에서 적절히 설계하기 어려운 경향이 있으며, 간섭이 증가하지 않습니다.
- 모든 AP에 대해 단일 채널 설정을 사용하는 것은 스캔 측면에서 좋은 방법입니다. 이는 지원할 총 클라이언트 수가 매우 낮고 대역폭 요구 사항이 높지 않은 경우에만 가능합니다. 이렇게 하면 검사 시간에서 무선 변경 시간이 제거됩니다. 이 옵션을 활용할 수 있는 환경은 거의 없으므로 주의하여 사용하십시오.
- 5.0GHz 대역의 경우, 로컬 규정에서 가능한 경우, WGB가 수동적인 수신 대신 각 채널을 능동적으로 탐색할 수 있으므로 DFS 이외의 실내 채널(36~48)을 사용하면 스캔 시간이 더 빠릅니다.

구축에 사용 중인 채널 계획은 다른 요구 사항을 수용해야 할 수 있습니다. 일반적인 RF 설계 권장 사항을 사용합니다.

스캔 채널 목록을 구성하려면

```
in d0
mobile station scan 1 6 11
```

참고: 모바일 스테이션은 라디오에서 WGB 역할을 사용할 때만 표시됩니다.

참고: WGB 스캔 목록이 인프라 채널 목록과 일치하는지 확인하십시오. 그렇지 않으면 WGB에서 사용 가능한 AP를 찾지 못합니다.

타이머 구성

12.4(25a)JA부터 문제가 발견되면 복구 타이머를 최적화하는 몇 가지 새로운 명령이 있습니다. 이 명령은 AP가 WGB 모드에 있을 때만 사용할 수 있습니다.

```
wgb-1260(config)#workgroup-bridge timeouts ?
```

```
assoc-response  Association Response time-out value
auth-response   Authentication Response time-out value
client-add      client-add time-out value
eap-timeout     EAP Timeout value
iapp-refresh    IAPP Refresh time-out value
```

assoc-response, auth-response, client-add의 경우 WGB가 부모 AP가 응답할 때까지 기다리는 시간을 나타내며, AP를 dead(데드)로 간주하고 다음 후보를 시도합니다. 기본값은 5초이며, 일부 응용 프로그램에서는 너무 깁니다. 최소 타이머는 800ms이며 대부분의 모바일 애플리케이션에 권장됩니다.

eap-timeout에서 WGB는 전체 EAP 인증 프로세스가 완료될 때까지 최대 대기 시간을 설정합니다. EAP 인증자가 응답하지 않을 경우 프로세스를 다시 시작하기 위해 EAP 신청자 POV에서 작동합니다. 기본값은 60초입니다. 전체 802.1x 인증을 완료하는 데 필요한 실제 시간보다 낮은 값을 구성하지 않도록 주의하십시오. 일반적으로 이 값을 2초에서 4초로 설정하는 것이 대부분의 구축에 적합합니다.

iapp-refresh의 경우 WGB는 기본적으로 로밍 후 상위 AP에 대한 IAPP 대량 업데이트를 생성하여 알려진 유선 클라이언트를 알립니다. 약 10초 후에 연동 후에 두 번째 재전송이 있습니다. 이 타이머를 사용하면 연결 후 IAPP 대량 중 "빠른 재시도"를 수행하여 첫 번째 IAPP 업데이트가 RF로 인해 손실되었거나 상위 AP에 아직 설치되지 않은 암호화 키를 극복할 수 있습니다. 빠른 로밍 시나리오의 경우 100ms를 사용할 수 있습니다. 그러나 WGB가 많이 사용되고 있는지 확인합니다. 따라서 각 로밍 후 인프라로 전송된 총 IAPP 수가 크게 증가합니다.

집계 값의 예:

```
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

이 테스트는 모바일 WGB 구축 시나리오에서 성공적으로 테스트되었습니다.

기타 WGB 최적화

WGB 구축 시나리오에 대해 고려해야 할 다른 사소한 변경 사항이 있습니다.

무선 관련

- rts 재시도 감소 - rts 재시도 32회. 이렇게 하면 종합 시나리오에서 일부 RF 시간을 절약할 수 있습니다. 일반적으로 이것은 필요하지 않습니다.
- 안테나 유형: 단일 안테나를 사용하는 경우(다양성 없음) 일반 성능을 향상하도록 라디오를 구성해야 합니다.

```
antenna transmit right-a
antenna receive right-a
```

안테나 다이버시티는 바람직하지만 차량에 안테나를 물리적으로 설치할 때 항상 가능한 것은 아닙니다. 로밍에는 적절한 안테나를 선택해야 합니다. 평균 로밍 시간에 2dB만 있으면 큰 차이가 날 수 있습니다.

관련 로그

- 밀리초를 절약하려면 콘솔 로깅 레벨을 오류로만 줄입니다. **콘솔 오류 로깅**. 일부 조건에서 로밍 성능에 부정적인 영향을 미칠 수 있으므로 완전히 비활성화하지 마십시오.
- 디버깅 또는 로그를 수집하려면 이더넷 측에서 텔넷 또는 ssh를 사용하는 것이 좋습니다. 이는 콘솔을 통한 디버깅 로깅과 비교하여 성능에 미치는 영향이 훨씬 적습니다. **로깅 모니터 디버깅**.
- WGB 로밍 POV에 대해 발생하는 사항을 이해하는 명령은 **debug dot11 dot11 0 추적 인쇄 업 링크**입니다. 이는 CPU에 미치는 영향이 적지만, 각 디버그 옵션이 총 로밍 시간을 늘릴 수 있으므로 지침이 없는 한 다른 디버그 옵션을 활성화하지 마십시오.
- 가능하면 SNTP를 사용하십시오. 이렇게 하면 WGB 시간이 동기화 상태로 유지되므로 문제 해결에 매우 유용합니다.

MFP 사용

- MFP는 보안 관점에서 유용할 수 있습니다. 그러나 로밍 실패 시나리오에서 WGB는 어떤 이유로든 둘 사이의 암호화 키가 잘못되었을 경우 AP 상위 키에서 새 로밍을 트리거하기 위해 AP 부모로부터 de-auth 프레임을 수락하지 않는다는 단점이 있습니다.
- 이러한 드문 실패 시나리오에서 현재 상위 항목이 RF 신호를 양호한 상태로 들릴 경우 WGB가 새 검사를 트리거하는 데 최대 5초가 걸릴 수 있습니다. 이 시간 동안 유효한 데이터 프레임을 수신하지 못할 경우 WGB에서 트리거할 수 있는 "모두 탐지" 메커니즘이 있습니다.
- 기본적으로 SSID에 WPA2 AES가 사용 중인 경우 WGB는 클라이언트 MFP를 사용하려고 시도합니다.
- 빠른 복구 시간이 필요한 경우 클라이언트 MFP를 비활성화하는 것이 좋습니다(보호되지 않는 인증 프레임에 반응하려면 WGB). 이는 보안 요구 사항과 신속한 복구 시간 사이에 절충되는 것입니다. 구축 시나리오에서 더 중요한 사항에 따라 결정됩니다.

```
dot11 ssid wgbpsk
no ids mfp client
```

WGB의 EAP-TLS 및 "시계 저장 간격"

[Cisco IOS Release 12.4\(21a\)JY용 Cisco Aironet Access Points and Bridges의 릴리스 정보의 Synchronize IOS Supplicant Clocks and Save Time Setting to NVRAM\(IOS 서플리컨트 클과 시간을 NVRAM으로 동기화\) 섹션을 참조하십시오.](#)

uWGB를 사용하는 경우, 일반적으로 연결된 MAC 주소와 연결되어 있고 uWGB BVI에는 네트워크 액세스가 없기 때문에 uWGB는 SNTP 동기화를 수행할 수 없습니다. 따라서 uWGB의 경우 최소 구축 시 NVRAM에서 올바른 클럭 동기화를 가져오는 것이 좋습니다. 연결된 Net 디바이스에서 NTP 소스(및 uWGB 연결을 통해 업데이트된 클라이언트)가 될 수 있는 기능이 있는 경우, uWGB sntp 동기화를 유효한 NTP 리플렉션 포인트로 간주할 수 있습니다.

전체 구성 예

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname wgb-1260
!
logging rate-limit console 9
logging console errors
!
clock timezone CET 1
no ip domain lookup
!
!
dot11 syslog
!
!
dot11 ssid wgbpsk
    vlan 32
    authentication open
    authentication key-management wpa version 2
    wpa-psk ascii 7 060506324F41584B56
    no ids mfp client
!
!
!
!
!
!
username Cisco password 7 13261E010803
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid wgbpsk
!
antenna transmit right-a
antenna receive right-a
    packet retries 32
station-role workgroup-bridge
rts retries 32
mobile station scan 2412 2437 2462
mobile station minimum-rate 6.0
mobile station period 3 threshold 70
bridge-group 1
!

interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
!
```

```
interface BVI1
ip address 192.168.32.67 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.32.1
no ip http server
no ip http secure-server

bridge 1 route ip

snmp server 192.168.32.1
clock save interval 1
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

디버그 분석

문제가 발생하는 경우 **debug dot11 dot11 0 trace print uplink** 명령의 출력을 첫 번째 단계로 캡처하는 것이 중요합니다. 이렇게 하면 로밍 프로세스에서 발생하는 상황을 잘 볼 수 있습니다.

다음은 현재 상위 후보입니다.

```
Sep 27 11:42:38.797: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio0, parent lost: Signal strength too low
```

```
Sep 27 11:42:38.797: CDD051F1-0 Uplink: Lost AP, Signal strength too low
```

낮은 신호 충족에 대한 트리거입니다. 모바일 스테이션 기간 X threshold Y 명령에 따라 달라집니다. 첫 번째 메시지는 항상 콘솔로 전송되며, 두 번째 메시지는 업링크 디버그 추적의 일부입니다. 이는 문제가 아니라 일반적인 WGB 프로세스의 일부입니다.

```
Sep 27 11:42:38.798: CDD052C7-0 Uplink: Wait for driver to stop
```

업링크 프로세스에서는 채널 스캔을 시작하기 전에 무선 대기열 비우기를 강제로 실행합니다. 이 단계는 채널 사용률 및 대기열 깊이에 따라 밀리초~몇 초 정도 걸릴 수 있습니다. 데이터 프레임이 시간 초과되지 않았습니까. 음성 프레임은 시간 비교가 이루어지므로 더 빨리 삭제해야 합니다. 시끄러운 환경에서는 약간의 지연이 발생할 수 있습니다.

```
Sep 27 11:42:38.798: CDD05371-0 Uplink: Enabling active scan
```

```
Sep 27 11:42:38.799: CDD05386-0 Uplink: Scanning
```

실제 채널 스캔이 수행됩니다. 구성된 채널당 약 10~13ms의 라디오를 주차합니다.

```
Sep 27 11:42:38.802: CDD064CD-0 Uplink: Rcvd response from 0021.d835.ade0 channel 1 3695
```

받은 프로브 응답 목록입니다. 첫 번째 숫자는 채널이고, 두 번째는 수신하는 데 걸린 마이크로초입니다.

```
Sep 27 11:42:38.808: CDD078F1-0 Uplink: Compare1 0021.d835.ade0 - Rssi 58dBm, Hops 0, Count 0, load 0
```

```
Sep 27 11:42:38.809: CDD07929-0 Uplink: Compare2 0021.d835.cce0 - Rssi 46dBm, Hops 0, Count 0, load 0
```

다음 세부 정보에서 수행된 실제 비교:

Sep 27 11:42:38.809: CDD07BDB-0 Uplink: Same as previous, send null data packet

상위 선택

Sep 27 11:42:38.809: CDD07BF7-0 Uplink: Done

Sep 27 11:42:38.808: %DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0, Associated To AP AP1 0021.d835.ade0 [None WPAv2 PSK]Roaming completed.

로밍이 "완료"되는 지점입니다. IAPP 프레임이 부모에 의해 처리되는 즉시 트래픽이 재개됩니다.

상위 비교 정보

Sep 27 14:16:47.590: F515B1FF-0 Uplink: Compare1 0021.d835.7620 - Rssi 60dBm, Hops 0, Count 0, load 3

Sep 27 14:16:47.591: F515B238-0 Uplink: Compare2 0021.d835.e8b0 - Rssi 58dBm, Hops 0, Count -1, load 0

compare1은 "현재" AP가 여전히 하나의 WGB에 연결되어 있는 경우 실제 연결 수 -1을 인쇄합니다 (따라서 WGB 자체는 숫자에서 사용되지 않음). 그러면 실제 흡과 로드입니다.

compare2는 차이점을 인쇄합니다. 그래서 음수를 볼 수 있다. 테스트의 숫자가 전류보다 크면 음수가 표시됩니다.

현재 연결 수, 로드, 신호 차이, 모바일 임계값 값에 따라 WGB가 새 부모를 선택할 수도 있고 선택하지 않을 수도 있습니다.

비교는 항상 두 AP 간에 이루어지며, 선택한 AP가 다음 반복의 현재 AP를 대체합니다. 따라서 일부 결정은 한 루프의 RSSI 때문이거나 다음 테스트의 다른 요인 때문일 수 있습니다.

관련 정보

- [Cisco Unified Wireless 네트워크에서 EAP-TLS 인증과 함께 IOS WGB를 사용하는 방법](#)
- [기술 지원 및 문서 - Cisco Systems](#)