

LWAPP 트래픽 연구

목차

[소개](#)

[설정](#)

[LWAPP 제어 채널](#)

[초기/일회성 교환](#)

[지속적인 교환](#)

[LWAPP 데이터](#)

[프레임 패딩](#)

[조각화](#)

[결론](#)

[관련 정보](#)

소개

CAPWAP(Control And Provisioning of Wireless Access Points) 작업 그룹에 제출된 IETF-RFC 초안은 LWAPP(Light Weight Access Point Protocol)를 무선 종료 지점(액세스 포인트)과 액세스 컨트롤러(무선 LAN 컨트롤러) 간의 통신 지침을 정의하는 것을 목표로 개발된 프로토콜로 설명합니다. 모든 LWAPP 통신은 다음 두 메시지 유형 중 하나로 분류될 수 있습니다.

- LWAPP 제어 채널
- LWAPP 캡슐화된 데이터

LWAPP는 레이어 2 또는 레이어 3 전송 모드에서 작동할 수 있습니다.레이어 2 LWAPP 통신은 이더넷 프레임으로 캡슐화되며 이더 타입 값 0x88BB로 식별할 수 있습니다.이더넷의 안정성 때문에 레이어 2 LWAPP 작동 모드는 라우팅할 수 없으며 WLC와 AP 간에 레이어 2 가시성이 필요합니다.레이어 2는 더 이상 사용되지 않는 것으로 간주되며, 이 트래픽 연구에 설명된 프로토콜 통계는 레이어 3 LWAPP 전송 모드를 기반으로 합니다.레이어 3 LWAPP 전송 모드는 IP 네트워크에서 UDP 캡슐화된 패킷 형식으로 LWAPP 메시지를 교환하도록 지정합니다.LWAPP 터널은 WLC(ap-manager) 인터페이스의 IP 주소 및 AP의 IP 주소로 유지됩니다.이 트래픽 조사에서는 LWAPP 메시지가 네트워크에 존재하는 실제 오버헤드의 양과 표준 설치에서 LWAPP 작업의 베이스라인을 보여줍니다.

참고: LWAPP 사양은 LWAPP-IETF [초안](#)에서 자세히 [설명합니다](#).

설정

이 문서는 LWAPP의 작동과 관련된 통계와 컨트롤러 간 로밍과 같이 프로토콜 사양에 의해 정의되지 않은 모든 기능이 이 문서의 범위를 벗어납니다.또한 트래픽 연구는 LWAPP 작업의 레이어 3 모드만 다룹니다.

그림 1:LWAPP 트래픽 연구 설정

LWAPP-Traffic Study

- AP sends a "Discovery Request" frame to the WLC
- WLC sends a "Discovery Response" frame
- AP sends a "Join Request" frame
- WLC sends the "Join Response" frame
- WLC and AP exchange configuration parameters*
- AP is enabled for operation

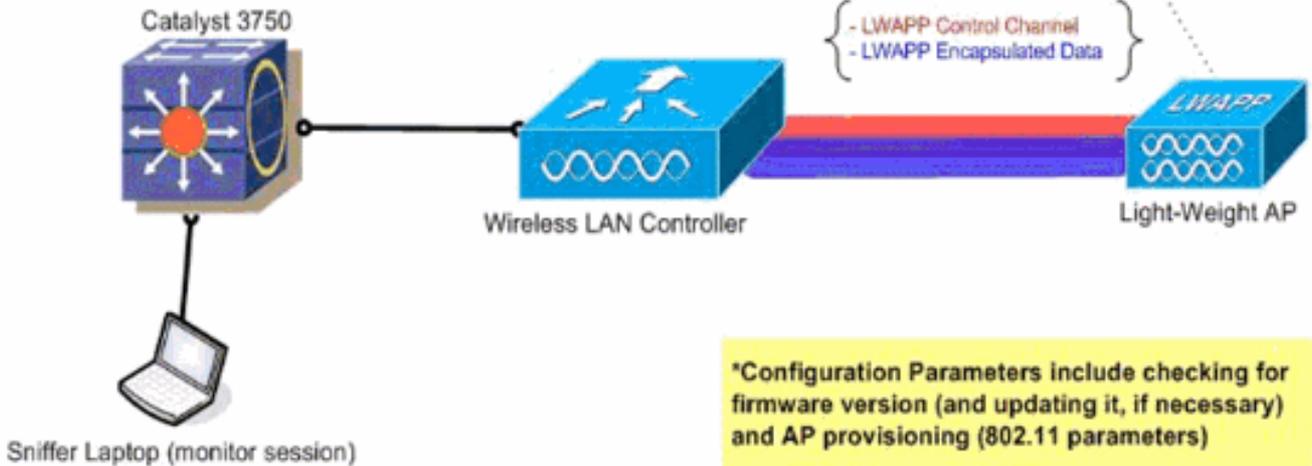


표 1: LWAPP 트래픽 조사 관련 장치의 참조 IP 주소

인터페이스/디바이스	IP 주소
WLC - 관리 인터페이스	192.168.10.102
WLC - ap-manager 인터페이스	192.168.10.103
경량 AP	192.168.10.22

이 트래픽 연구를 위해 초기 교환 및 컨피그레이션 변경 기준을 설정하기 위해 액세스 포인트가 하나만 포함된 설정이 생성되었습니다. 나중에 더 많은 AP가 추가되어 AP 수를 줄여서 와이어에서 생성된 트래픽 양에 미치는 영향을 확인했습니다.

LWAPP 제어 채널

AP는 WLC와 통신할 때 임시 포트를 사용합니다. WLC에서 사용하는 포트 번호는 LWAPP Data 및 LWAPP Control 트래픽의 UDP 포트 12222 및 UDP 포트 12223입니다. LWAPP 컨트롤 프레임은 LWAPP의 헤더 플래그 필드에 있는 "C" 비트로 LWAPP 데이터 프레임과 구별됩니다. 1로 설정하면 컨트롤 프레임입니다.

초기/일회성 교환

LWAPP 검색(요청 및 응답)

그림 2: LWAPP 검색 요청 및 응답 패킷 흐름

Time	192.168.10.22	192.168.10.102	255.255.255.255	192.168.10.103	Comment
100.090	(54419)	LWAPP	(12223)		CNTL DISCOVERY_REQUEST
100.090	(54419)	LWAPP	(12223)		CNTL DISCOVERY_REQUEST
100.091	(54419)	LWAPP	(12223)		CNTL DISCOVERY_REPLY
100.091	(54419)	LWAPP	(12223)		CNTL DISCOVERY_REPLY

액세스 포인트가 보낸 LWAPP 검색 요청은 네트워크에 어떤 WLC가 있는지 확인하기 위해 사용됩니다.

검색 요청 패킷은 97바이트이며, 여기에는 4바이트 FCS가 포함됩니다. 검색 응답 패킷은 106바이트이며, 여기에는 4바이트 FCS가 포함됩니다.

LWAPP 가입(요청 및 응답)

그림 3:LWAPP 가입 요청 및 응답 패킷 흐름

Time	192.168.10.22	192.168.10.102	255.255.255.255	192.168.10.103	Comment
112.274	(54419)	LWAPP	(12223)		CNTL JOIN_REQUEST
112.371	(54419)	LWAPP	(12223)		CNTL JOIN_REPLY

LWAPP 가입 요청 패킷은 컨트롤러를 통해 클라이언트를 서비스할 것임을 WLC에 알리기 위해 액세스 포인트에서 사용됩니다. 또한 전송 시 지원되는 MTU를 검색하는 데 조인 요청 단계가 사용됩니다. 액세스 포인트에서 보낸 초기 조인 요청은 항상 1596바이트의 테스트 요소로 채워집니다. AP와 컨트롤러 간의 전송 설정 방식에 따라 이러한 조인 요청 프레임도 프래그먼트화될 수 있습니다. 초기 요청에 대한 조인 응답이 수신되면 AP는 조각화 없이 프레임을 전달합니다. 조인 응답은 또한 하트비트 타이머(30초 값)를 시작하며, 이 값은 만료되면 WLC-AP 세션을 삭제합니다. Echo Request 또는 Acknowledgement를 수신하면 타이머가 새로 고쳐집니다.

초기 조인 요청에서 어떤 응답도 생성하지 않을 경우 AP는 테스트 요소와 함께 다른 조인 요청을 보냅니다. 그러면 총 페이로드가 1500바이트로 이동됩니다. 두 번째 조인 요청도 응답을 생성하지 않을 경우 AP는 큰 패킷과 작은 패킷 사이에서 계속 순환하며 결국 검색 단계부터 다시 시작할 시간이 초과됩니다.

조인 요청 및 응답 메시지에 대한 패킷 크기는 설명에 따라 다르지만 AP와 WLC(ap-manager interface) 간의 이 트래픽 연구의 목적으로 캡처된 패킷 교환은 3,000바이트입니다.

LWAPP 구성

그림 4:LWAPP 상태 및 AP 프로비저닝 패킷 흐름 구성

Time	192.168.10.22	192.168.10.102	255.255.255.255	192.168.10.103	Comment
113.762	(54412)		LWAPP	(12223)	CNTL CONFIGURE_REQUEST
113.812	(54412)		LWAPP	(12223)	CNTL CONFIGURE_RESPONSE
113.814	(54412)		LWAPP	(12223)	CNTL CHANGE_STATE_EVENT
113.814	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND
113.819	(54412)		LWAPP	(12223)	CNTL CHANGE_STATE_EVENT_RES
113.891	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND_RES
113.891	(54412)		LWAPP	(12223)	CNTL CHANGE_STATE_EVENT
113.892	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND
113.893	(54412)		LWAPP	(12223)	CNTL CHANGE_STATE_EVENT_RES
113.894	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND_RES
113.894	(54412)		LWAPP	(12223)	CNTL CHANGE_STATE_EVENT
113.895	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND
113.896	(54412)		LWAPP	(12223)	CNTL CHANGE_STATE_EVENT_RES
113.896	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND_RES
113.897	(54412)		LWAPP	(12223)	CNTL CHANGE_STATE_EVENT
113.899	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND
113.899	(54412)		LWAPP	(12223)	CNTL CHANGE_STATE_EVENT_RES
113.901	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND_RES
113.901	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND
113.902	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND_RES
113.902	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND
113.903	(54412)		LWAPP	(12223)	CNTL CONFIGURE_COMMAND_RES
132.024	(54412)		LWAPP	(12223)	CNTL CHANGE_STATE_EVENT
132.025	(54412)		LWAPP	(12223)	CNTL CHANGE_STATE_EVENT_RES
132.026	(54412)		LWAPP	(12223)	CNTL CHANGE_STATE_EVENT

AP에서 제공하는 서비스를 생성, 변경(업데이트) 또는 삭제하기 위해 액세스 포인트와 컨트롤러 간에 LWAPP 컨피그레이션 요청 및 응답이 교환됩니다.

일반적으로 AP는 현재 컨피그레이션을 WLC로 전송하기 위해 요청 구성 메시지를 보냅니다.

구성 요청은 두 가지 시나리오에서 전송할 수 있습니다.

1. AP가 컨트롤러에 연결되고 컨트롤러에 구성된 모든 802.11 설정으로 프로비저닝해야 하는 초기 단계에서
2. 온디맨드 관리 변경(예: WLAN 매개변수 변경)

AP에서 LWAPP 컨피그레이션 요청 수신을 확인하기 위해 WLC에서 AP로 LWAPP 컨피그레이션 응답 메시지 유형을 전송합니다. 그러면 WLC가 AP의 요청된 컨피그레이션을 재정의할 수 있습니다. 이러한 프레임에 포함된 특수 메시지 요소가 없습니다.

AP와 WLC(ap-manager interface) 간의 초기 교환은 약 6,000바이트에 해당되며 1회 컨피그레이션 변경의 평균은 360바이트이며 WLC의 AP 및 ap-manager 인터페이스에서 각각 2개의 패킷이 포함됩니다.

RRM(Radio Resource Management)

그림 5:초기 RRM 패킷 흐름

Time	192.168.10.22	192.168.10.102	255.255.255.255	192.168.10.103	Comment
132.028	(54419) ←	LWAPP		(12223)	CNTL RRM_CONTROL_REQ
132.028	(54419)	LWAPP		(12223) →	CNTL RRM_CONTROL_RES
132.029	(54419) ←	LWAPP		(12223)	CNTL RRM_CONTROL_REQ
132.029	(12223) ←	LWAPP		(54419)	CNTL RRM_CONTROL_RES
132.029	(12223)	LWAPP		(54419) →	CNTL RRM_CONTROL_REQ
132.030	(12223) ←	LWAPP		(54419)	CNTL RRM_CONTROL_RES
132.030	(12223)	LWAPP		(54419) →	CNTL RRM_CONTROL_REQ
132.031	(12223) ←	LWAPP		(54419)	CNTL RRM_CONTROL_RES
132.031	(12223)	LWAPP		(54419) →	CNTL RRM_CONTROL_REQ
132.032	(54419)	LWAPP		(12223) →	CNTL RRM_CONTROL_RES
132.032	(54419) ←	LWAPP		(12223)	CNTL RRM_CONTROL_REQ
132.033	(54419)	LWAPP		(12223) →	CNTL RRM_CONTROL_RES
132.033	(54419) ←	LWAPP		(12223)	CNTL RRM_CONTROL_REQ
132.033	(54419)	LWAPP		(12223) →	CNTL RRM_CONTROL_RES
132.034	(54419) ←	LWAPP		(12223)	CNTL RRM_CONTROL_REQ
132.034	(12223) ←	LWAPP		(54419)	CNTL RRM_CONTROL_RES
132.035	(12223)	LWAPP		(54419) →	CNTL RRM_CONTROL_REQ
132.035	(54419)	LWAPP		(12223) →	CNTL RRM_CONTROL_RES

AP가 프로비저닝되면 RRM 관련 정보 교환이 이루어집니다. AP와 WLC(ap-manager 인터페이스) 간의 일반적인 교환은 약 1,400바이트입니다. RRM 관련 컨피그레이션이 변경될 경우 WLC의 AP와 ap-manager 인터페이스 간에 4개의 패킷 교환이 이루어집니다. 이 교환은 평균 375바이트입니다.

검색, 조인, 컨피그레이션 및 진행 중인 프로세스를 포함하는 20분 샘플 캡처는 100Mbps 세그먼트에서 다음과 같은 트래픽 통계를 생성했습니다.

표 1:단일 액세스 포인트에 대한 초기 LWAPP 트래픽 통계

통계	가치
총 바이트	84,869
평균 사용률(퍼센트)	0.001
평균 사용률(킬로비트/초)	0.425
최대 사용률(퍼센트)	0.004
최대 사용률(킬로비트/초)	5.384

그림 6은 전체 프로세스를 그림으로 나타낸 것입니다.

그림 6:AP 검색, 가입 및 프로비저닝 단계 중 프로토콜 비교

Protocol	Percentage	Bytes	Packets
Ethernet Type 2	0.000%	0	0
IP	0.000%	0	0
UDP	0.000%	0	0
LWAPP	0.000%	0	0
LWAPP Control	75.170%	10,057	52
BOOTP	0.000%	0	0
DHCP	14.470%	1,936	4
IP Fragment	5.576%	746	2
ARP	0.000%	0	0
Response	2.392%	320	5
Request	1.913%	256	4
Loopback	0.478%	64	1

지속적인 교환

하트비트

LWAPP 아키텍처는 일련의 **에코 요청** 및 **에코 응답**에 의해 수행되는 하트비트 타이머를 제공합니다. AP는 AP와 WLC 간의 연결 상태를 확인하기 위해 정기적으로 에코 요청을 전송합니다. 이에 대한 응답으로 WLC는 에코 요청 수신을 확인하기 위해 에코 응답을 전송합니다. 그런 다음 AP에서 하트비트 타이머를 EchoInterval로 **재설정**합니다. LWAPP 프로토콜 사양 초안에는 이러한 타이머에 대한 자세한 설명이 포함되어 있습니다. 시스템 하트비트는 대체 메커니즘과 결합되어 30초마다 4개의 패킷이며 다음 패킷으로 구성됩니다.

```
LWAPP ECHO_REQUEST from AP (78 bytes)
LWAPP Echo-Response to AP (64 bytes)
LWAPP PRIMARY_DISCOVERY_REQ from AP (93 bytes)
LWAPP Primary Discovery-Response to AP (97 bytes)
```

이 교환은 30초마다 33바이트의 트래픽을 생성합니다.

RRM 측정

두 가지 RRM 교환이 진행 중입니다. 60초 간격마다 첫 번째 값은 로드 및 신호 측정이며 4개의 패킷으로 구성됩니다. 이 Exchange는 항상 최대 396바이트를 추가합니다.

```
LWAPP RRM_DATA_REQ from AP (107 bytes)
LWAPP Airewave-Director-Data Response to AP (64 bytes)
LWAPP RRM_DATA_REQ from AP (161 bytes)
LWAPP Airewave-Director-Data Response to AP (64 bytes)
```

두 번째 패킷 시퀀스는 통계 정보 요청 및 응답 시퀀스를 포함하는 노이즈 측정입니다. 180초마다 수행됩니다. 이 짧은 패킷 교환은 평균 약 2,660바이트이며 일반적으로 0.01초입니다. 이 패킷은 다음 패킷으로 구성됩니다.

```
LWAPP RRM_DATA_REQ from AP
LWAPP Airewave-Director-Data Response to AP
LWAPP RRM_DATA_REQ from AP
LWAPP Airewave-Director-Data Response to AP
LWAPP RRM_DATA_REQ from AP
LWAPP Airewave-Director-Data Response to AP
LWAPP RRM_DATA_REQ from AP
LWAPP Airewave-Director-Data Response to AP
```

LWAPP STATISTICS_INFO from AP
 LWAPP Statistics-Info Response to AP

LWAPP RRM_DATA_REQ from AP
 LWAPP Airewave-Director-Data Response to AP
 LWAPP RRM_DATA_REQ from AP
 LWAPP Airewave-Director-Data Response to AP
 LWAPP RRM_DATA_REQ from AP 00:14:1b:59:41:80
 LWAPP Airewave-Director-Data Response to AP
 LWAPP RRM_DATA_REQ from AP
 LWAPP Airewave-Director-Data Response to AP

LWAPP STATISTICS_INFO from AP
 LWAPP Statistics-Info Response to AP

비인가 측정

비인가 측정은 검사 메커니즘의 일부로 수행되며 180초마다 RRM 교환에 포함됩니다. 자세한 내용은 [Unified Wireless Networks 아래의 무선 리소스 관리](#)를 참조하십시오.

20분 샘플 캡처는 100Mbps 세그먼트의 지속적인 패킷 교환에 대해 다음 값을 가져왔습니다.

표 2: 단일 액세스 포인트에 대한 지속적인 LWAPP 트래픽 통계

통계	가치
총 바이트	45,805
평균 사용률(퍼센트)	< 0.001
평균 사용률(킬로비트/초)	0.35
최대 사용률(퍼센트)	< 0.001
최대 사용률(킬로비트/초)	0.002

표 2의 통계 및 교환은 다음 이미지에 나와 있습니다.

그림 7: AP가 정상적으로 작동하는 동안 프로토콜 비교 20분 샘플

Protocol	Percentage	Bytes	Packets
Ethernet Type 2	0.000%	0	0
IP	0.000%	0	0
UDP	0.000%	0	0
LWAPP	0.000%	0	0
LWAPP Control	75.173%	34,433	334
LWAPP Data	22.312%	10,220	80
ARP	0.000%	0	0
Response	2.515%	1,152	18

그림 8: LWAPP 컨트롤 대 LWAPP 데이터 트래픽 바이트 값 비교

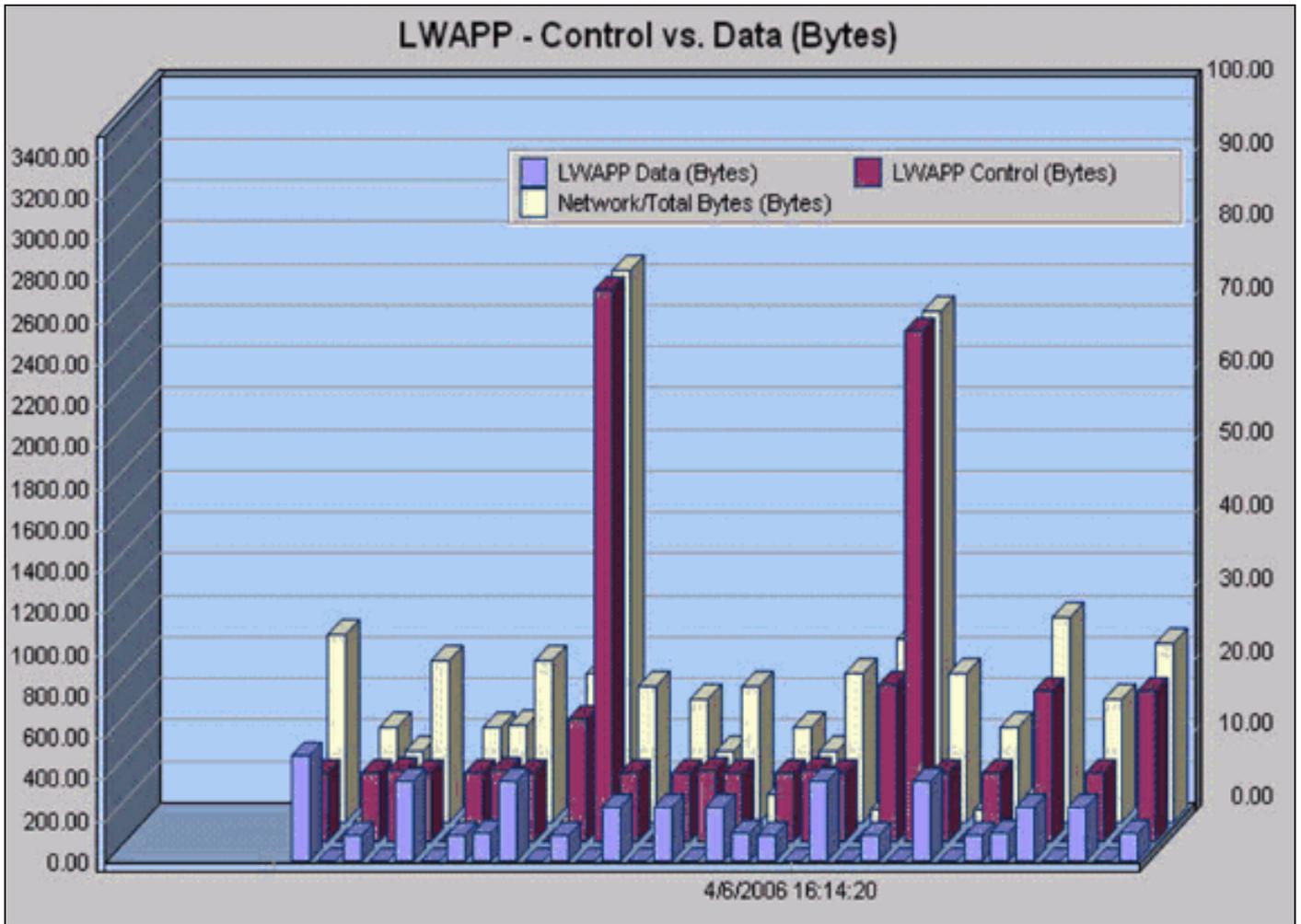
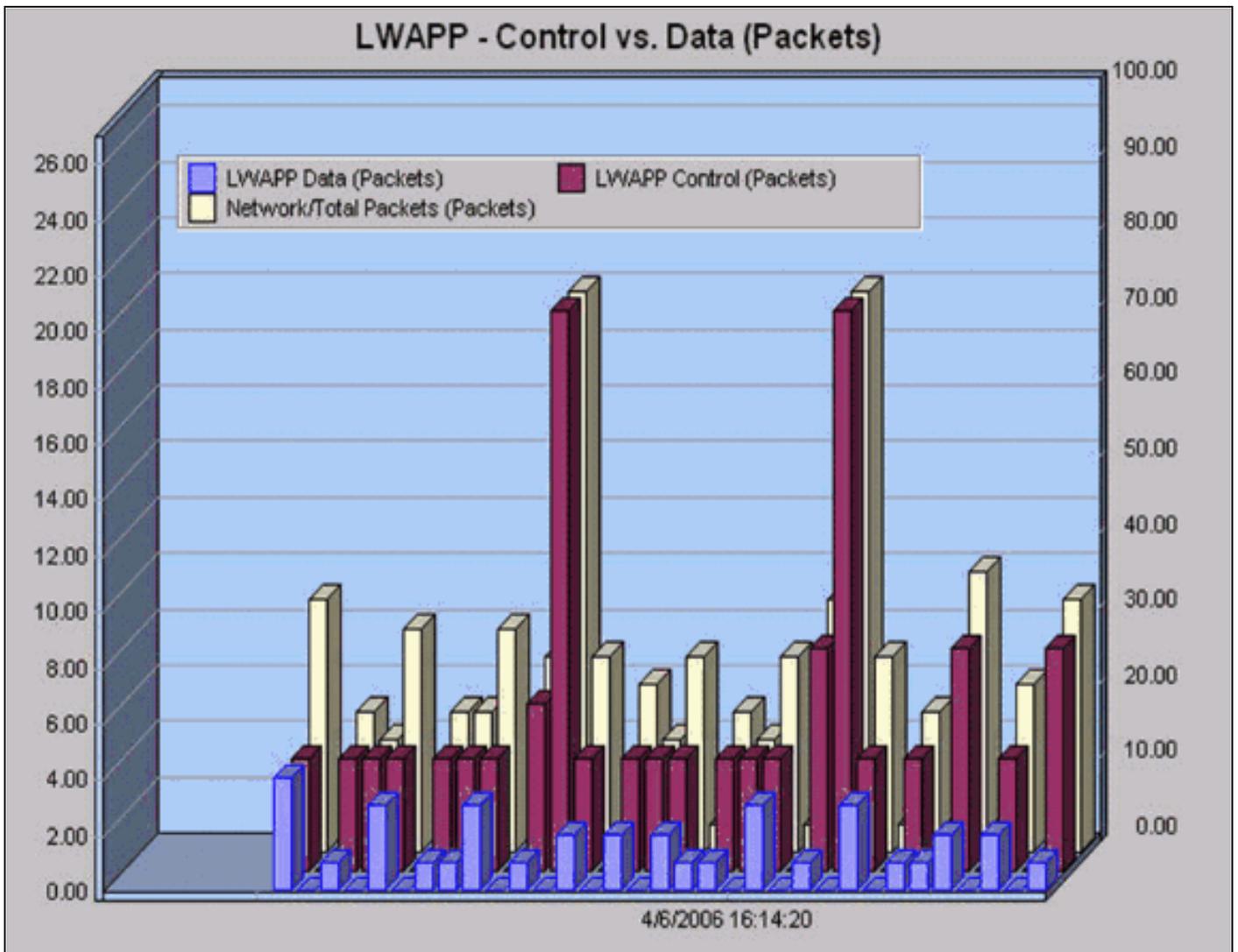


그림 9: LWAPP 제어 대 LWAPP 데이터 트래픽 패킷 수 비교



LWAPP 데이터

프레임 패딩

LWAPP 데이터 프레임 헤더는 기존 802.11 패킷에 6바이트를 추가합니다. 이 헤더는 캡슐화된 802.11 프레임 앞에 추가되며 다음을 포함합니다.

Light Weight Access Point Protocol [0-40]

```

Flags:                %00000000 [42-48]
00.. .. . . . . . . . . Version: 0
..00 0... Radio ID: 0
.... .0.. C Bit - Data message [0-29]
.... ..0. F Bit - Fragmented packet [0-34]
.... ...0 L Bit - Last fragment [0-30]
  
```

```

Fragment ID:         0x00 [43-55]
Length:              74 [44-52]
Rec Sig Strngth Indic:183 dBm [46-77]
Signal to Noise Ratio:25 dB [47-76]
  
```

조각화

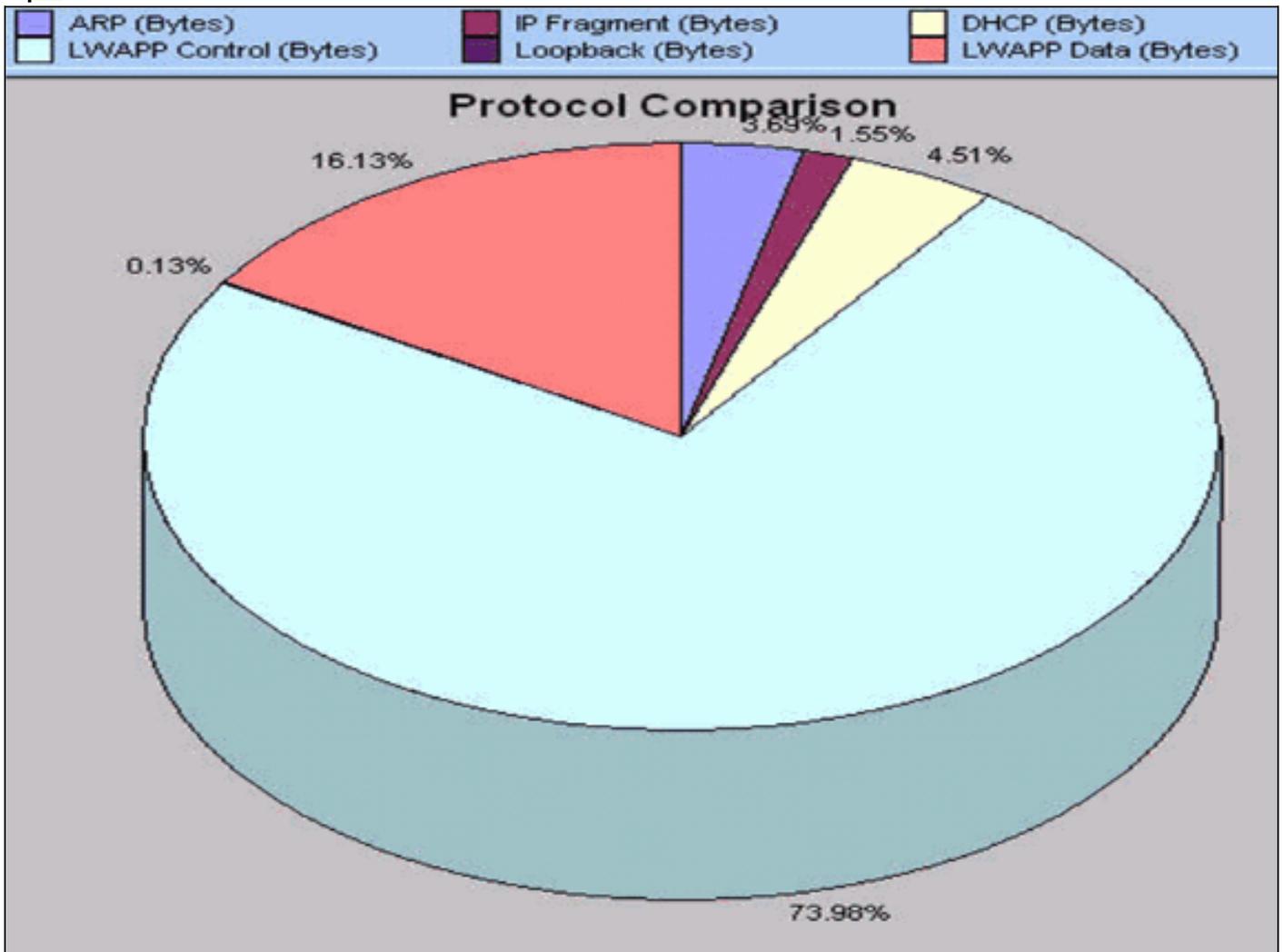
LWAPP 프레임은 프래그먼트화될 수 있으므로 Fragment ID 필드가 포함됩니다. 원래 프레임과 IP 프래그먼트를 추가하면 총 패킷 크기를 확인할 수 있습니다. IP 프래그먼트는 LWAPP 헤더에 캡슐화되지 않습니다.

결론

이 트래픽 연구에서 밝혀진 바에 따르면, LWAPP의 작동은 인프라에 과도한 대역폭 요구 사항을 야기하지 않으며, 대부분의 일반적인 구축에서는 Cisco Unified Wireless Architecture를 수용하기 위해 인프라에 추가 용량을 추가할 필요가 없습니다. 트래픽 조사의 요약으로서, LWAPP 운영에 대한 다음과 같은 빠른 사실을 염두에 둘 수 있습니다.

- 레이턴시가 중요한 고려 사항이지만, 이 트래픽 연구는 처리량 고려 사항만을 제시합니다. 일반적으로 AP-to-WLC 링크는 왕복 지연 시간을 100ms를 초과해서는 안 됩니다.
- LWAPP의 작동을 위한 두 개의 개별 채널이 있습니다. LWAPP 데이터 LWAPP 제어 트래픽
- LWAPP 작업은 두 가지 범주로 분류됩니다. 일회성 교환 지속적인 교환
- 초기 교환을 포함하는 20분 샘플의 경우 평균 활용률이 0.001%입니다.
- 진행 중인 교환의 20분 샘플의 경우 최대 활용률은 0.35킬로비트/초입니다.
- LWAPP 데이터 채널은 각 802.11 데이터 패킷에 6바이트의 헤더를 추가합니다. IP 프래그먼트에 대한 추가 오버헤드가 없습니다.
- 1시간 길이의 샘플에서는 프로토콜과 해당 백분율을 보여 줍니다.

그림 10: 낮은 데이터 트래픽, IP 프래그먼트 및 다수의 LWAPP을 포함한 1시간 캡처 기반 프로토콜 비교



관련 정보

- [WLC\(Wireless LAN Controller\)에 LAP\(Lightweight AP\) 등록](#)
- [LWAPP 기본 사항](#)
- [경량 AP\(LAP\)에서 LWAPP 컨피그레이션 재설정](#)
- [LWAPP 업그레이드 도구 문제 해결 팁](#)
- [기술 지원 및 문서 - Cisco Systems](#)