

LWAPP-Datenverkehrsstudie

Inhalt

[Einführung](#)

[Einrichtung](#)

[LWAPP-Kontrollkanal](#)

[Erstmaliger/einmaliger Austausch](#)

[Laufende Exchange](#)

[LWAPP-Daten](#)

[Rahmen](#)

[Fragmentierung](#)

[Fazit](#)

[Zugehörige Informationen](#)

Einführung

Der IETF-RFC-Entwurf, der der Arbeitsgruppe Control And Provisioning of Wireless Access Points (CAPWAP) vorgelegt wurde, beschreibt das Light Weight Access Point Protocol (LWAPP) als Protokoll, das entwickelt wurde, um Kommunikationsrichtlinien zwischen Wireless Termination Points (Access Points) und Access Controllern (Wireless LAN Controller) zu definieren. Alle LWAPP-Kommunikation kann in einen der beiden folgenden Meldungstypen klassifiziert werden:

- LWAPP-Kontrollkanal
- LWAPP-gekapselte Daten

LWAPP kann entweder im Layer-2- oder Layer-3-Transportmodus betrieben werden. Layer-2-LWAPP-Kommunikation ist in Ethernet-Frames gekapselt und kann mit einem EtherType-Wert von 0x88BB identifiziert werden. Aufgrund der Zuverlässigkeit auf Ethernet ist der Layer-2-LWAPP-Betriebsmodus nicht routingfähig und erfordert Layer-2-Transparenz zwischen den WLCs und APs. Layer 2 wird als veraltet angesehen, und die in dieser Datenverkehrsstudie skizzierten Protokollstatistiken basieren auf dem Layer-3-LWAPP-Transportmodus. Der Layer-3-LWAPP-Transportmodus gibt den Austausch von LWAPP-Nachrichten im IP-Netzwerk in Form von UDP-gekapselten Paketen an. Der LWAPP-Tunnel wird mit der IP-Adresse der WLC-Schnittstelle (ap-manager) und der IP-Adresse des AP verwaltet. Diese Datenverkehrsstudie zeigt die tatsächliche Menge an Overhead auf, die LWAPP-Nachrichten in einem Netzwerk verursachen, sowie eine Baseline für den LWAPP-Betrieb bei einer Standardinstallation.

Hinweis: Die LWAPP-Spezifikation wird ausführlich unter [LWAPP-IETF Draft](#) behandelt.

Einrichtung

Dieses Dokument enthält Statistiken, die sich nur auf den Betrieb von LWAPP beziehen, und alle Funktionen, die nicht in der Protokollspezifikation definiert sind, wie z. B. Roaming zwischen Controllern, fallen nicht in den Anwendungsbereich dieses Dokuments. Darüber hinaus umfasst

die Datenverkehrsstudie nur den Layer-3-Modus des LWAPP-Betriebs.

Abbildung 1: Einrichtung der LWAPP-Datenverkehrsstudie

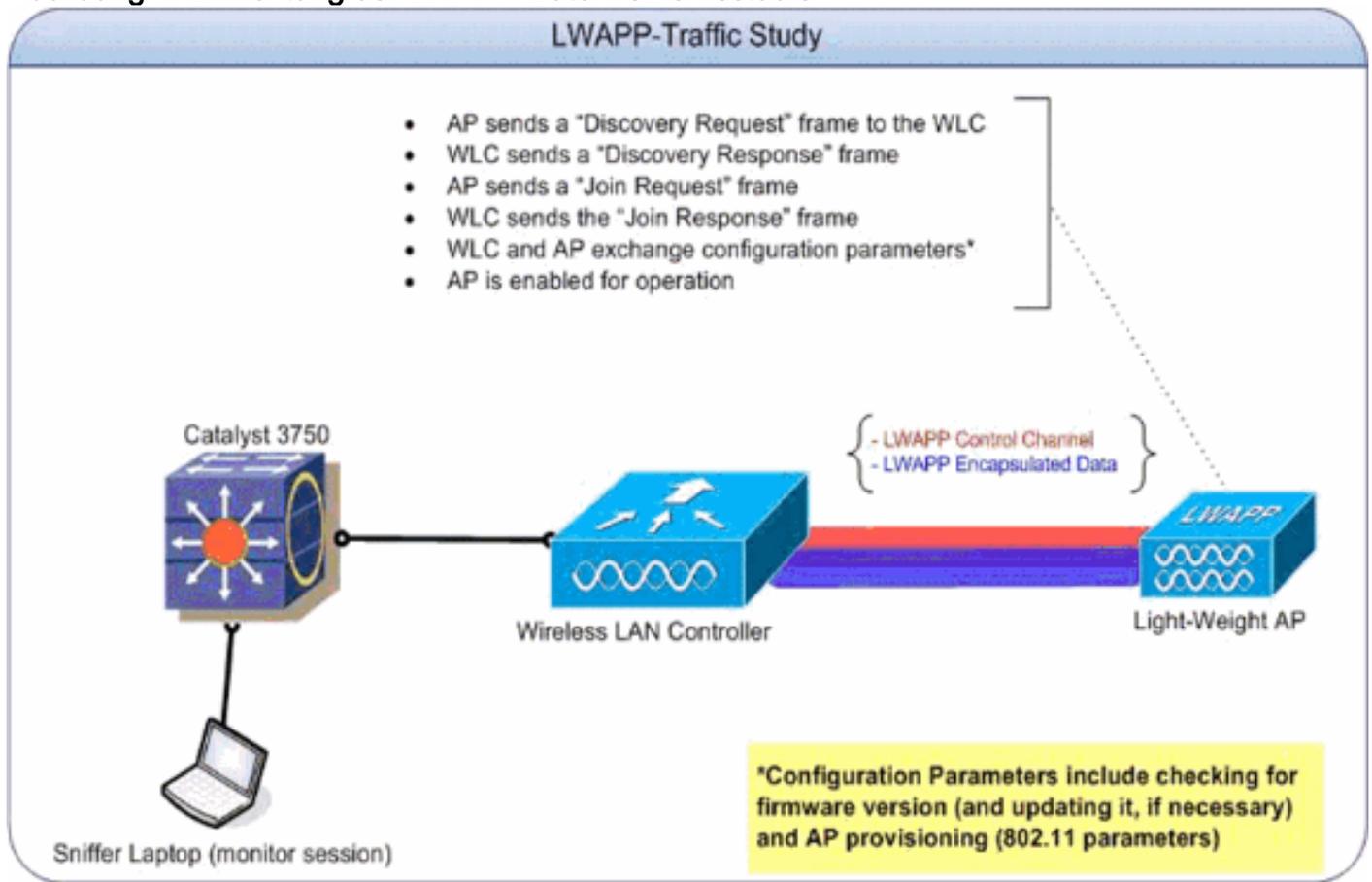


Tabelle 1: Referenzielle IP-Adressen für Geräte, die an LWAPP-Datenverkehrsstudien beteiligt sind

Schnittstelle/Gerät	IP-Adresse
WLC = Management Interface	192.168.10.102
WLC = ap-manager Interface	192.168.10.103
AP mit geringem Gewicht	192.168.10.22

Für diese Datenverkehrsstudie wurde die Einrichtung mit nur einem Access Point erstellt, um die Baselines für erste Austausch- und Konfigurationsänderungen festzulegen. Später wurden weitere Access Points hinzugefügt, um die Auswirkungen der Skalierung der Anzahl von Access Points auf die Menge des über die Leitung generierten Datenverkehrs zu ermitteln.

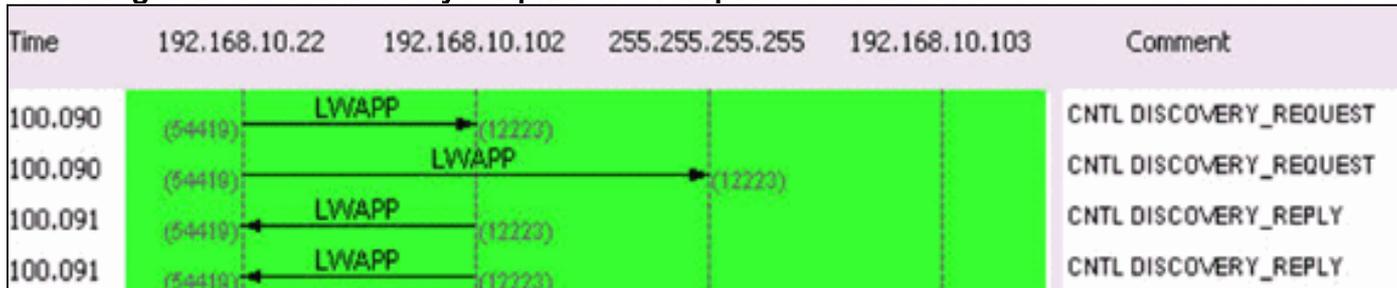
LWAPP-Kontrollkanal

Der WAP verwendet ephemere Ports, wenn er mit dem WLC kommuniziert. Die vom WLC verwendeten Portnummern sind dagegen der UDP-Port 1222 und der UDP-Port 12223 für LWAPP-Daten- bzw. der LWAPP-Kontrollverkehr. Ein LWAPP-Steuerelementrahmen unterscheidet sich von einem LWAPP-Datenrahmen durch das "C"-Bit im Header-Flag-Feld des LWAPP. Bei der Einstellung auf 1 handelt es sich um einen Kontrollrahmen.

Erstmaliger/einmaliger Austausch

[LWAPP Discovery \(Anforderung und Antwort\)](#)

Abbildung 2: LWAPP Discovery Request and Response Packet Flow

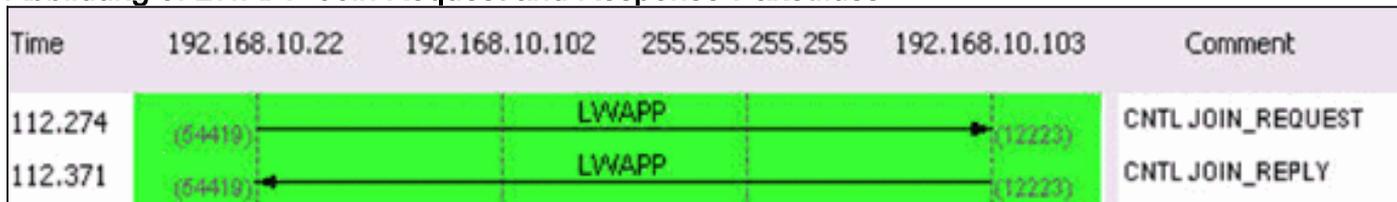


Die vom Access Point gesendeten LWAPP-Erkennungsanfragen dienen dazu, festzustellen, welche WLCs im Netzwerk vorhanden sind.

Ein Discovery Request-Paket beträgt 97 Byte, das den 4-Byte-FCS enthält. Ein Discovery-Response-Paket beträgt 106 Byte, das den 4-Byte-FCS enthält.

[Teilnahme an LWAPP \(Anfrage und Antwort\)](#)

Abbildung 3: LWAPP-Join Request and Response-Paketfluss



Ein LWAPP-Join-Request-Paket wird vom Access Point verwendet, um dem WLC mitzuteilen, dass er Clients über den Controller bedienen möchte. Die Join-Anforderungsphase wird auch verwendet, um die vom Transport unterstützte MTU zu ermitteln. Die erste Join-Anfrage, die vom Access Point gesendet wird, wird immer mit einem Testelement von 1596 Byte gepaart. Je nachdem, wie der Transport zwischen dem Access Point und dem Controller eingerichtet wird, können diese Verbindungsanforderungen auch fragmentiert werden. Wenn für die erste Anforderung eine Join-Antwort empfangen wird, leitet der Access Point Frames ohne Fragmentierung weiter. Die Join-Antwort initiiert außerdem den Heartbeat-Timer (ein 30-Sekunden-Wert), der nach Ablauf die WLC-AP-Sitzung löscht. Der Timer wird nach Erhalt der Echo Request oder Acknowledgement aktualisiert.

Wenn die erste Join-Anforderung keine Antwort liefert, sendet der Access Point eine weitere Join-Anfrage mit dem Testelement, wodurch die Gesamt-Payload auf 1.500 Byte steigt. Wenn die zweite Verbindungsanforderung auch keine Antwort liefert, setzt der Access Point den Zyklus zwischen den großen und den kleinen Paketen fort und endet schließlich mit dem Neustart von der Erkennungsphase.

Die Paketgrößen für die Join-Anforderung und die Antwortnachrichten variieren je nach Beschreibung, aber der für diese Datenverkehrsstudie zwischen dem AP und dem WLC (ap-manager-Schnittstelle) erfasste Paketaustausch beträgt 3.000 Byte.

[LWAPP-Konfiguration](#)

Abbildung 4: LWAPP Configure State und AP Provisioning Packet Flow

Time	192.168.10.22	192.168.10.102	255.255.255.255	192.168.10.103	Comment
113.762	(5412)		LWAPP	(1223)	CNTL CONFIGURE_REQUEST
113.812	(5412)		LWAPP	(1223)	CNTL CONFIGURE_RESPONSE
113.814	(5412)		LWAPP	(1223)	CNTL CHANGE_STATE_EVENT
113.814	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND
113.819	(5412)		LWAPP	(1223)	CNTL CHANGE_STATE_EVENT_RES
113.891	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND_RES
113.891	(5412)		LWAPP	(1223)	CNTL CHANGE_STATE_EVENT
113.892	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND
113.893	(5412)		LWAPP	(1223)	CNTL CHANGE_STATE_EVENT_RES
113.894	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND_RES
113.894	(5412)		LWAPP	(1223)	CNTL CHANGE_STATE_EVENT
113.895	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND
113.896	(5412)		LWAPP	(1223)	CNTL CHANGE_STATE_EVENT_RES
113.896	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND_RES
113.897	(5412)		LWAPP	(1223)	CNTL CHANGE_STATE_EVENT
113.899	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND
113.899	(5412)		LWAPP	(1223)	CNTL CHANGE_STATE_EVENT_RES
113.901	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND_RES
113.901	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND
113.902	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND_RES
113.902	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND
113.903	(5412)		LWAPP	(1223)	CNTL CONFIGURE_COMMAND_RES
132.024	(5412)		LWAPP	(1223)	CNTL CHANGE_STATE_EVENT
132.025	(5412)		LWAPP	(1223)	CNTL CHANGE_STATE_EVENT_RES
132.026	(5412)		LWAPP	(1223)	CNTL CHANGE_STATE_EVENT

Die LWAPP-Konfigurationsanforderungen und -antworten werden zwischen den Access Points und den Controllern ausgetauscht, um die von einem Access Point angebotenen Services zu erstellen, zu ändern (aktualisieren) oder zu löschen.

Im Allgemeinen sendet ein WAP eine Konfigurationsanfrage, um seine aktuelle Konfiguration an seinen WLC zu senden.

Die Konfigurationsanforderung kann in zwei Szenarien gesendet werden:

1. In der Anfangsphase, in der der Access Point einem Controller beitrifft und mit allen 802.11-Einstellungen bereitgestellt werden muss, die auf dem Controller konfiguriert sind.
2. Bei On-Demand-Verwaltungsänderungen, z. B. Änderung eines WLAN-Parameters

Der Typ der LWAPP-Konfigurationsantwort wird vom WLC an den AP gesendet, um den Erhalt der LWAPP-Konfigurationsanforderung vom AP zu bestätigen. Dies bietet dem WLC die Möglichkeit, die angeforderte Konfiguration des Access Points zu überschreiben. Ein solcher Frame enthält keine speziellen Nachrichtenelemente.

Der erste Austausch zwischen dem Access Point und dem WLC (ap-manager interface) beträgt

ca. 6.000 Byte, und eine einmalige Konfigurationsänderung beträgt durchschnittlich 360 Byte und umfasst jeweils 2 Pakete vom Access Point und der AP-Manager-Schnittstelle des WLC.

Radio Resource Management (RRM)

Abbildung 5: Initialer RRM-Paketfluss

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

Ein RRM-bezogener Informationsaustausch findet statt, sobald der Access Point bereitgestellt wurde. Ein typischer Austausch zwischen dem Access Point und dem WLC (ap-manager interface) beträgt ca. 1.400 Byte. Im Falle einer Konfigurationsänderung im Zusammenhang mit dem RRM erfolgt ein 4-Paket-Austausch zwischen dem AP und der AP-Manager-Schnittstelle des WLC. Dieser Austausch beträgt im Durchschnitt 375 Byte.

Eine 20-minütige Beispielerfassung, die Erkennung, Verknüpfung, Konfiguration und laufende Prozesse umfasst, führte zu diesen Datenverkehrsstatistiken für ein 100-Mbit/s-Segment:

Tabelle 1: Ausgangsstatistiken des LWAPP-Datenverkehrs für einen einzelnen Access Point

Statistik	Wert
Byte gesamt	84,869
Durchschnittliche Auslastung (Prozent)	0.001
Durchschnittliche Auslastung (Kilobit/s)	0.425
Max. Auslastung (Prozent)	0.004
Max. Auslastung (Kilobit/s)	5.384

Abbildung 6 ist eine bildliche Darstellung des gesamten Prozesses.

Abbildung 6: Protokollvergleich während der Phase der AP-Erkennung, -Verbindung und -Bereitstellung

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

Laufende Exchange

Herzschlag

Die LWAPP-Architektur bietet einen Heartbeat-Timer, der durch eine Reihe von **Echo-Anfragen** und **Echo-Antworten** erreicht wird. Ein Access Point sendet regelmäßig Echoanfragen, um den Zustand der Verbindung zwischen dem Access Point und dem WLC zu ermitteln. Daraufhin sendet der WLC die Echo-Antwort, um den Empfang der Echo-Anforderung zu bestätigen. Der Access Point setzt dann den Heartbeat-Timer auf das **EchoInterval** zurück. Der LWAPP-Protokollspezifikationsentwurf enthält eine detaillierte Beschreibung dieser Timer. Der System-Heartbeat umfasst zusammen mit dem Fallback-Mechanismus 4 Pakete alle 30 Sekunden und besteht aus folgenden Paketen:

```
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)
```

Dieser Austausch generiert 33 Byte Datenverkehr alle 30 Sekunden.

RRM-Messungen

Es gibt zwei laufende RRM-Austausche. Die erste besteht in jedem Intervall von 60 Sekunden aus der Last und dem Signal und besteht aus 4 Paketen. Dieser Austausch hat immer eine Größe von 396 Byte:

```
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)
```

Die zweite Paketsequenz ist die Rauschmessung, die eine Statistikanforderung und eine Antwortsequenz beinhaltet. Dies erfolgt alle 180 Sekunden. Dieser kurze Datenaustausch dauert im Durchschnitt ca. 2.660 Byte und dauert in der Regel 0,01 Sekunden. Es besteht aus den folgenden Paketen:

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

Nicht autorisierte Messwerte

Nicht autorisierte Messwerte werden als Teil des Scan-Mechanismus durchgeführt und alle 180 Sekunden in den RRM-Austausch integriert. Weitere Informationen finden Sie unter [Unified Wireless Networks](#) unter Radio Resource Management.

Die 20-minütige Beispielerfassung führte zu den folgenden Werten für den laufenden Paketaustausch auf einem 100-Mbit/s-Segment:

Tabelle 2: Laufende LWAPP-Datenverkehrsstatistiken für einen einzelnen Access Point

Statistik	Wert
Byte gesamt	45,805
Durchschnittliche Auslastung (Prozent)	< 0,001
Durchschnittliche Auslastung (Kilobit/s)	0.35
Max. Auslastung (Prozent)	< 0,001
Max. Auslastung (Kilobit/s)	0.002

Die Statistiken und der Austausch in Tabelle 2 sind in folgenden Bildern dargestellt:

Abbildung 7: Eine 20-minütige Protokollvergleichsprobe während des normalen Betriebs des Access Points

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

Abbildung 8: LWAPP Control vs. LWAPP Datenverkehrsbytewerte verglichen

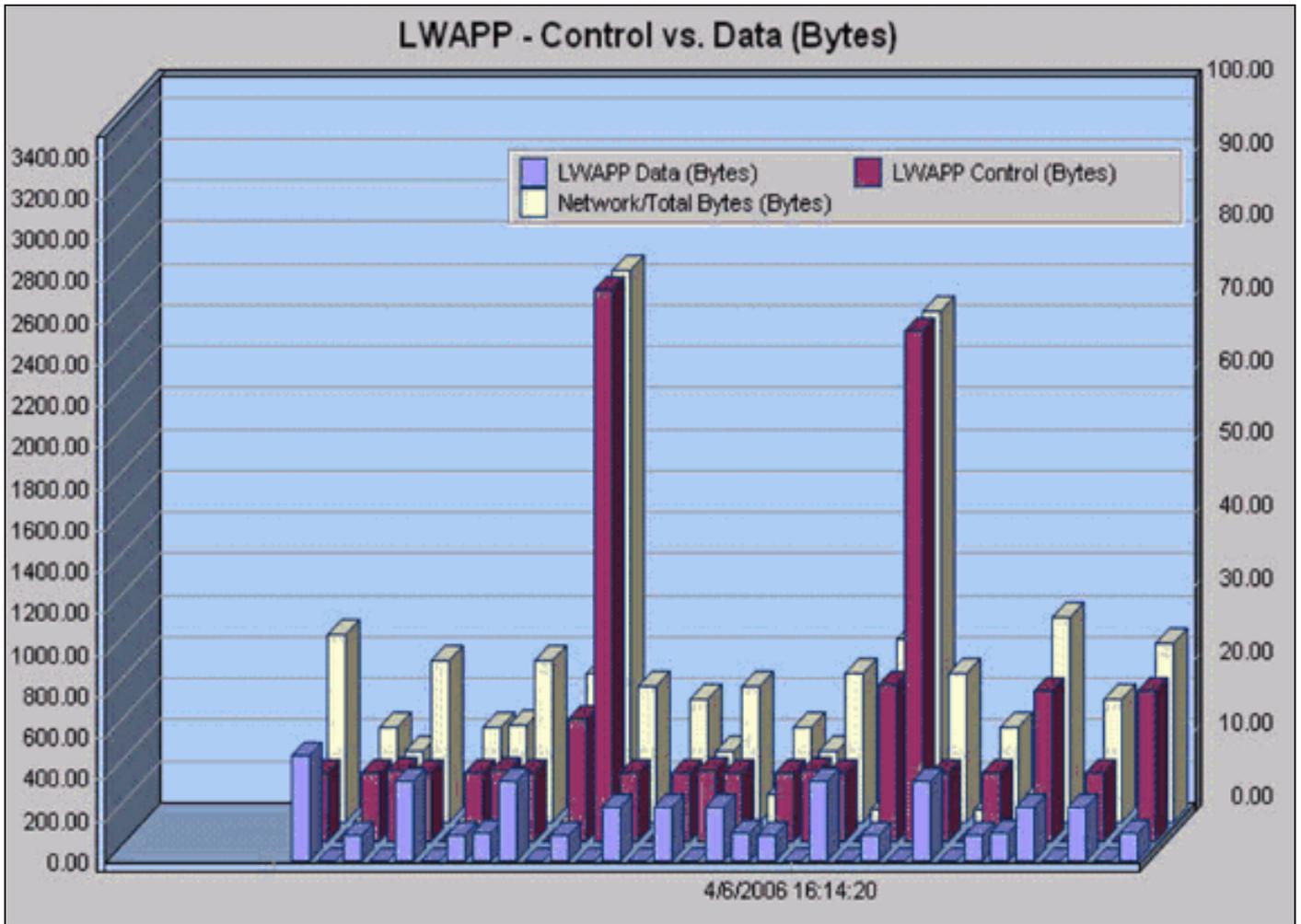
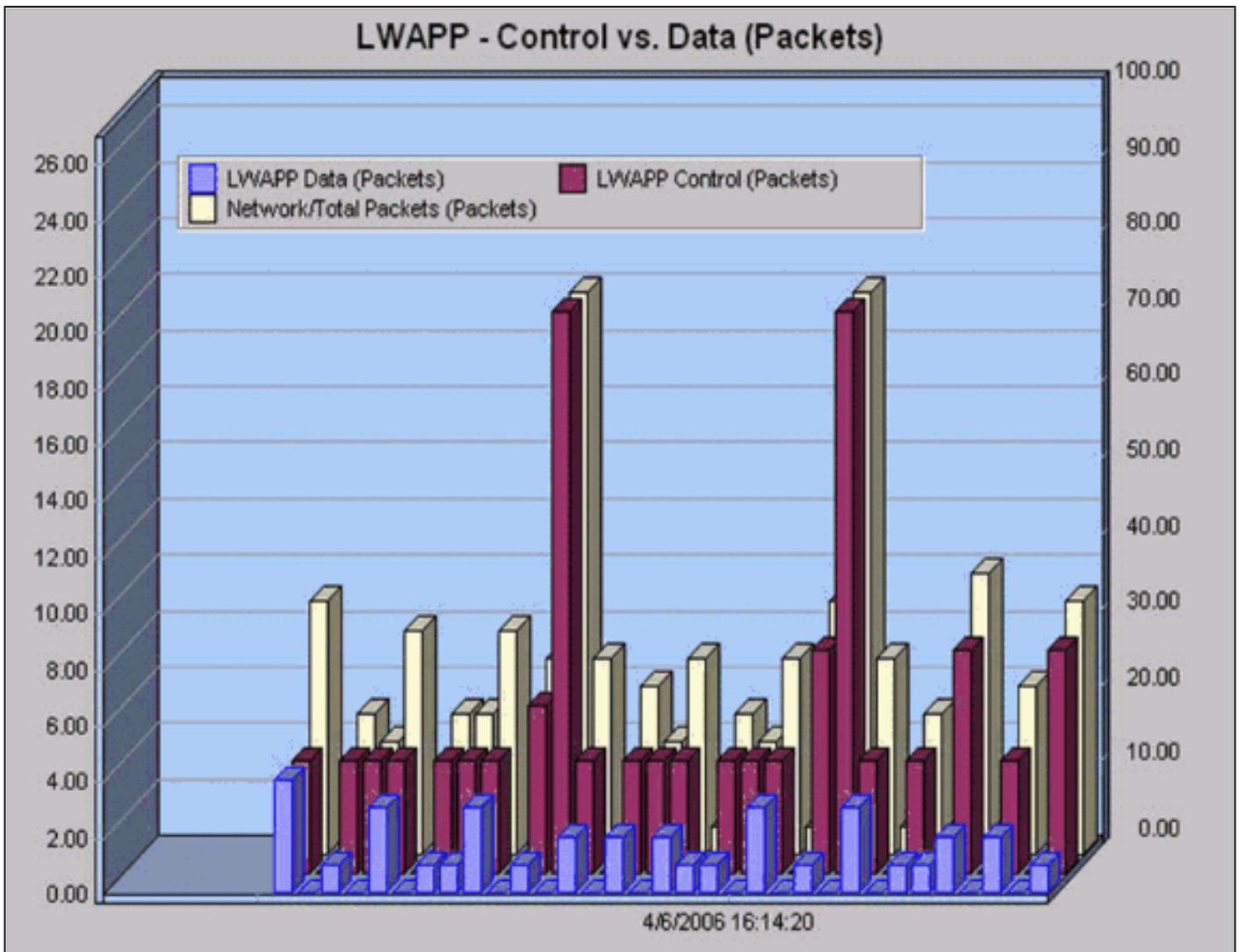


Abbildung 9: Vergleich LWAPP Control Vs LWAPP Datenverkehrspaketanzahl



LWAPP-Daten

Rahmen

Der LWAPP-Daten-Frame-Header fügt den vorhandenen 802.11-Paketen 6 Byte hinzu. Dieser Header wird vor dem gekapselten 802.11-Frame hinzugefügt und umfasst Folgendes:

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]

```

Fragmentierung

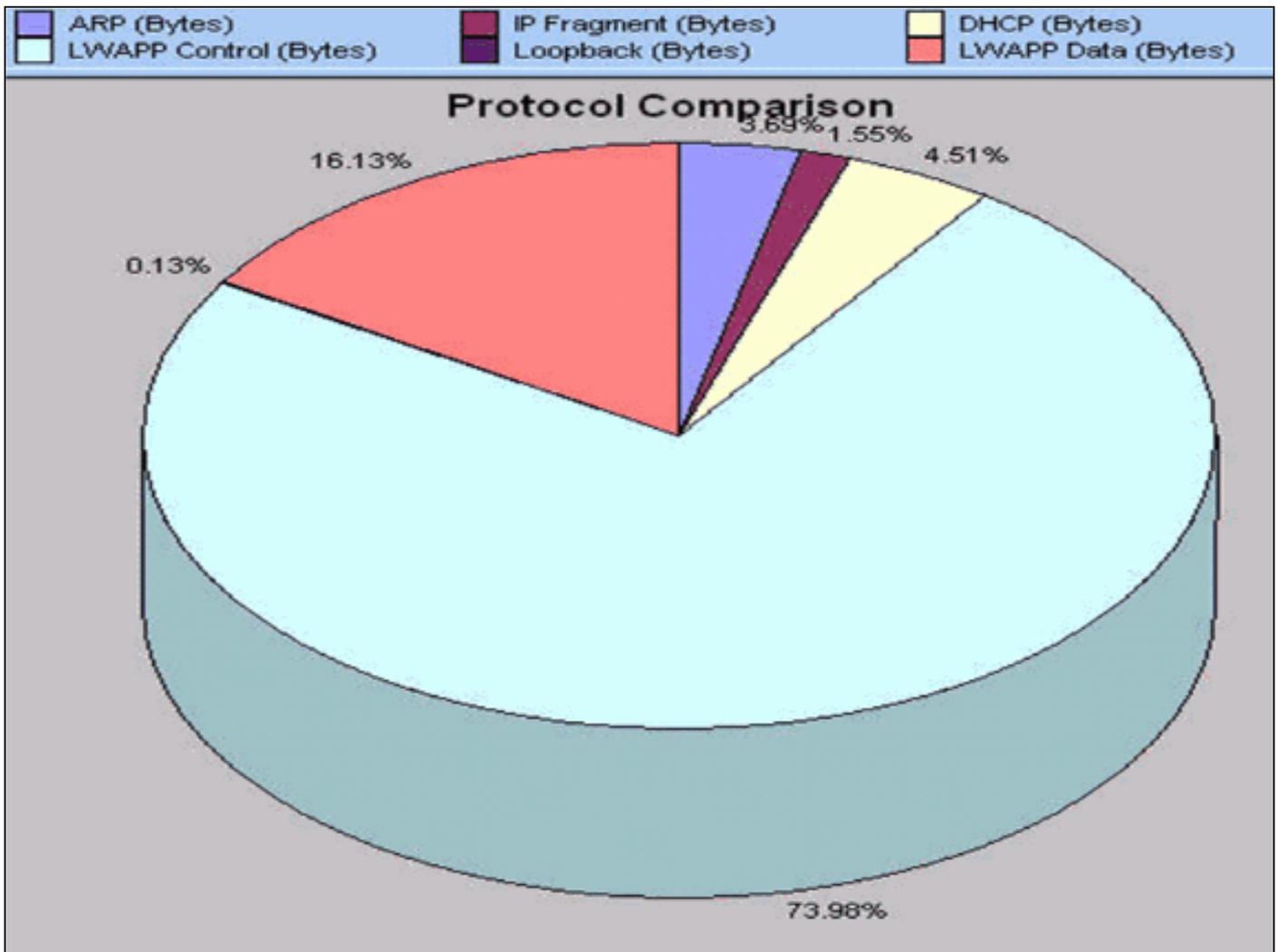
Da LWAPP-Frames fragmentiert werden können, ist ein Fragment-ID-Feld enthalten. Die Gesamtpaketgröße kann bestimmt werden, wenn Sie den ursprünglichen Frame und das IP-Fragment hinzufügen. Beachten Sie, dass das IP-Fragment nicht in LWAPP-Headern eingekapselt ist.

Fazit

Die Ergebnisse dieser Datenverkehrsstudie zeigen, dass der Betrieb von LWAPP keine hohen Bandbreitenanforderungen an die Infrastruktur mit sich bringt. In den meisten typischen Bereitstellungen ist keine zusätzliche Kapazität erforderlich, um die Cisco Unified Wireless Architecture zu unterstützen. Eine Zusammenfassung der Datenverkehrsstudie: Diese schnellen Fakten über den Betrieb von LWAPP sind zu beachten:

- Obwohl Latenz ein wichtiger Aspekt ist, werden in dieser Datenverkehrsstudie nur Durchsatzüberlegungen dargestellt. Als allgemeine Richtlinie darf die Round-Trip-Latenz von AP zu WLC 100 ms nicht überschreiten.
- Für den Betrieb von LWAPP gibt es zwei separate Kanäle: LWAPP-Daten LWAPP-Kontrolldatenverkehr
- Der LWAPP-Betrieb ist in zwei große Kategorien unterteilt: einmalige Börsenlaufende Börsen
- Eine 20-minütige Stichprobe, die den ersten Austausch umfasst, ergibt eine durchschnittliche Nutzungsstatistik von 0,001 Prozent.
- Eine 20-minütige Stichprobe laufender Börsen ergibt eine maximale Nutzungsstatistik von 0,35 Kilobit/Sekunde.
- Der LWAPP-Datenkanal fügt jedem 802.11-Datenpaket einen Header von 6 Byte hinzu. Für IP-Fragmente gibt es keinen zusätzlichen Overhead.
- In einem einstündigen Beispiel werden diese Aufspaltung von Protokollen und ihre jeweiligen prozentualen Anteile dargestellt:

Abbildung 10: Protokollvergleich basierend auf einer einstündigen Erfassung mit geringem Datenverkehr, IP-Fragmenten und mehrheitlich LWAPP



Zugehörige Informationen

- [Lightweight AP \(LAP\)-Registrierung bei einem Wireless LAN Controller \(WLC\)](#)
- [Grundlagen von LWAPP](#)
- [Zurücksetzen der LWAPP-Konfiguration auf einem Lightweight AP \(LAP\)](#)
- [Tipps zur Fehlerbehebung beim LWAPP-Upgrade-Tool](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)