

# Studio sul traffico LWAPP

## Sommario

[Introduzione](#)

[Configurazione](#)

[Canale di controllo LWAPP](#)

[Scambi iniziali/occasionali](#)

[Scambi in corso](#)

[Dati LWAPP](#)

[Spaziatura interna frame](#)

[Frammentazione](#)

[Conclusioni](#)

[Informazioni correlate](#)

## Introduzione

La bozza IETF-RFC, presentata al gruppo di lavoro Controllo e provisioning dei punti di accesso wireless (CAPWAP), descrive il protocollo LWAPP (Light Weight Access Point Protocol) come un protocollo sviluppato con l'obiettivo di definire linee guida per la comunicazione tra i punti di terminazione wireless (punti di accesso) e i controller di accesso (controller LAN wireless). Tutte le comunicazioni LWAPP possono essere classificate in uno di questi due tipi di messaggi:

- Canale di controllo LWAPP
- Dati incapsulati LWAPP

LWAPP può funzionare in modalità di trasporto di livello 2 o 3. Le comunicazioni LWAPP di layer 2 sono incapsulate in frame Ethernet e possono essere identificate con un valore EtherType di 0x88BB. A causa della sua affidabilità su Ethernet, la modalità di funzionamento LWAPP di layer 2 non è instradabile e richiede la visibilità di layer 2 tra i WLC e gli AP. Il layer 2 è considerato deprecato e le statistiche del protocollo descritte in questo studio sul traffico si basano sulla modalità di trasporto LWAPP del layer 3. La modalità di trasporto LWAPP di layer 3 specifica lo scambio di messaggi LWAPP sulla rete IP sotto forma di pacchetti incapsulati UDP. Il tunnel LWAPP viene gestito con l'indirizzo IP dell'interfaccia WLC (ap-manager) e l'indirizzo IP dell'access point. Questo studio sul traffico rivela la quantità effettiva di sovraccarico che i messaggi LWAPP presentano su una rete e una linea di base del funzionamento di LWAPP in un'installazione standard.

**Nota:** la specifica LWAPP è illustrata in dettaglio nella [bozza LWAPP-IETF](#).

## Configurazione

Questo documento presenta statistiche relative solo al funzionamento di LWAPP e qualsiasi funzionalità non definita dalla specifica del protocollo, ad esempio il roaming tra controller, non rientra nell'ambito del presente documento. Inoltre, lo studio sul traffico riguarda solo la modalità

layer 3 del funzionamento di LWAPP.

Figura 1: Impostazione di LWAPP Traffic Study

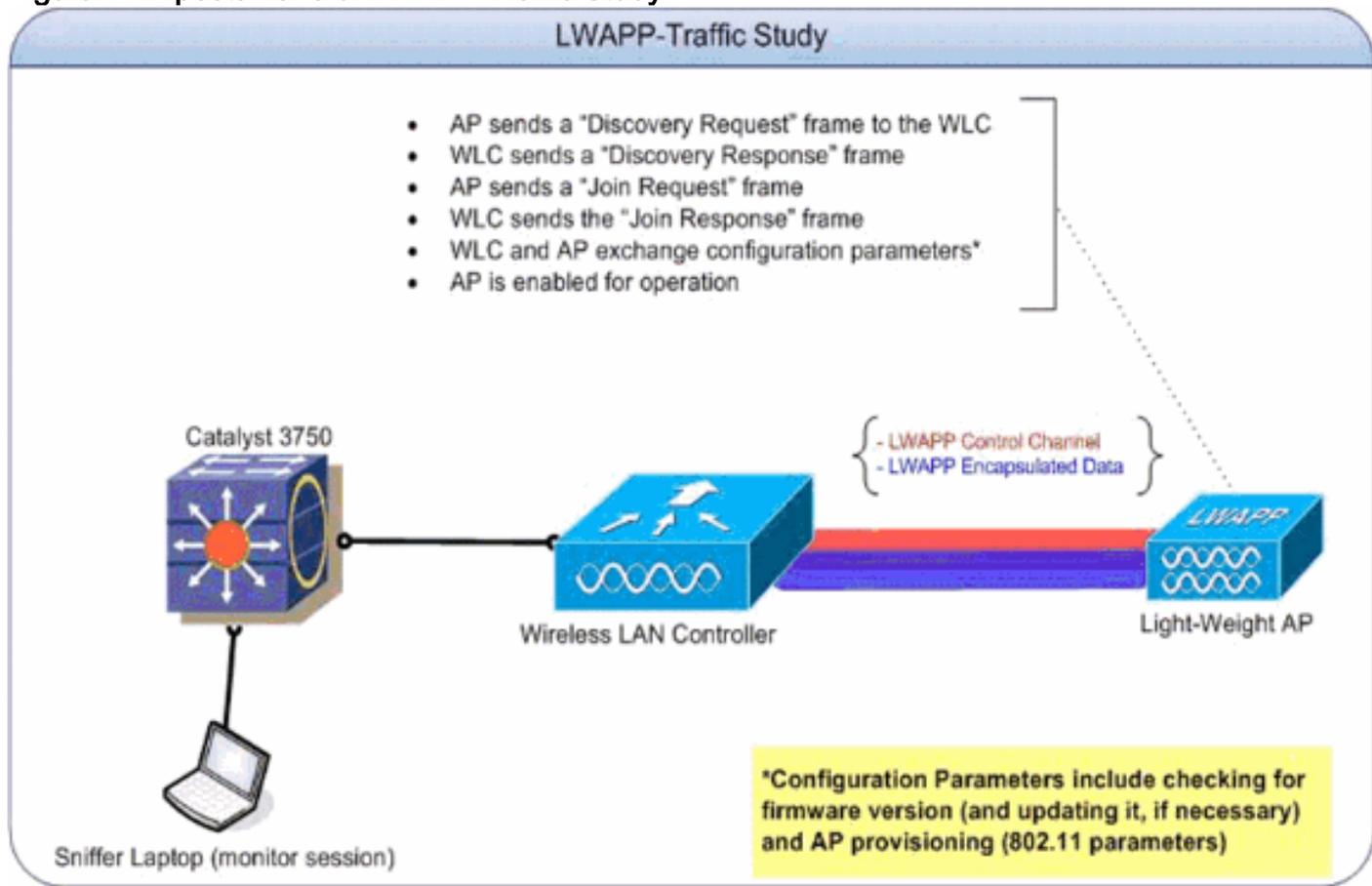


Tabella 1. Indirizzi IP referenziali per i dispositivi coinvolti nello studio sul traffico LWAPP

Interfaccia/Dispositivo	Indirizzo IP
WLC - Interfaccia di gestione	192.168.10.102
WLC - interfaccia ap-manager	192.168.10.103
Punto di accesso disattivo	192.168.10.22

Ai fini di questo studio sul traffico, la configurazione è stata creata con un solo punto di accesso per stabilire le baseline di modifica dello scambio iniziale e della configurazione. Successivamente sono stati aggiunti altri access point per determinare gli effetti della modifica in scala del numero di access point sulla quantità di traffico generata sul cavo.

## Canale di controllo LWAPP

L'AP utilizza le porte effimere quando comunica con il WLC. I numeri di porta utilizzati dal WLC, in cambio, sono rispettivamente la porta UDP 1222 e la porta UDP 1223 per il traffico LWAPP Data e il traffico LWAPP Control. Un frame di controllo LWAPP si distingue da un frame di dati LWAPP per il bit "C" nel campo flag dell'intestazione di LWAPP. Se impostato su 1, è un frame di controllo.

## Scambi iniziali/occasional

### Individuazione LWAPP (richiesta e risposta)

**Figura 2: Flusso di pacchetti di richiesta e risposta di individuazione LWAPP**

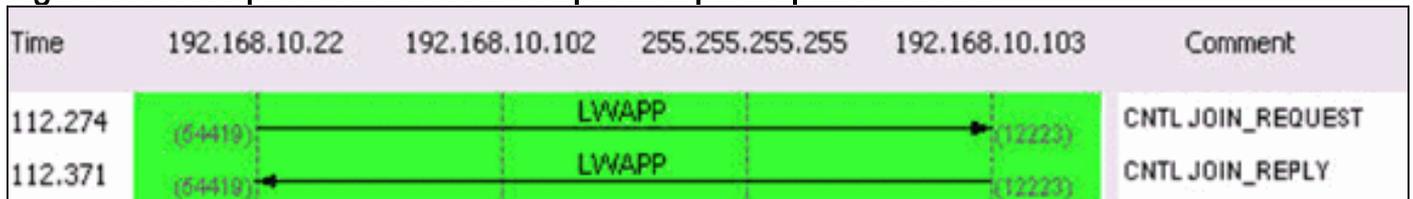


Le richieste LWAPP Discovery, inviate dal punto di accesso, vengono usate per determinare i WLC presenti nella rete.

Un pacchetto di richiesta di individuazione è di 97 byte, inclusi i FCS da 4 byte. Un pacchetto di risposta di individuazione è di 106 byte, inclusi i FCS da 4 byte.

### [Join LWAPP \(richiesta e risposta\)](#)

**Figura 3: Flusso pacchetti richiesta e risposta di partecipazione LWAPP**



Un pacchetto di richiesta di unione LWAPP viene utilizzato dal punto di accesso per informare il WLC che desidera servire i client tramite il controller. La fase di richiesta di join viene usata anche per trovare l'MTU supportata dal trasporto. La richiesta di join iniziale inviata dal punto di accesso viene sempre riempita con un elemento di test di 1596 byte. A seconda della configurazione del trasporto tra l'access point e il controller, è possibile frammentare anche questi frame di richiesta di join. Se viene ricevuta una risposta di join per la richiesta iniziale, l'access point inoltra i frame senza alcuna frammentazione. La risposta join avvia anche il timer di heartbeat (un valore di 30 secondi) che, quando scade, elimina la sessione WLC-AP. Il timer viene aggiornato alla ricezione della richiesta echo o delle conferme.

Se la richiesta di join iniziale non restituisce alcuna risposta, l'access point invia un'altra richiesta di join con l'elemento di test, che porta il payload totale a 1500 byte. Se anche la seconda richiesta di join non restituisce una risposta, l'access point continua a spostarsi tra i pacchetti grandi e piccoli e alla fine scade per ricominciare dalla fase di individuazione.

Le dimensioni dei pacchetti per i messaggi di richiesta di unione e di risposta variano in base alla descrizione, ma lo scambio di pacchetti acquisito ai fini di questo studio sul traffico tra l'AP e il WLC (interfaccia del gestore dell'access point) è di 3.000 byte.

### [Configurazione LWAPP](#)

**Figura 4: LWAPP Configura lo stato e il flusso del pacchetto di provisioning AP**

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

Le richieste e le risposte di configurazione LWAPP vengono scambiate tra i punti di accesso e i controller per creare, modificare (aggiornare) o eliminare i servizi offerti da un access point.

In generale, un messaggio Configure Request viene inviato da un access point per inviare la configurazione corrente al proprio WLC.

La richiesta di configurazione può essere inviata in due scenari:

1. Nella fase iniziale, quando l'access point si unisce a un controller e deve essere configurato con tutte le impostazioni 802.11 configurate sul controller.
2. In caso di modifiche amministrative su richiesta, come la modifica di un parametro WLAN

Il tipo di messaggio di risposta della configurazione LWAPP viene inviato dal WLC all'access point per confermare la ricezione della richiesta di configurazione LWAPP dall'access point. Ciò consente al WLC di ignorare la configurazione richiesta dall'access point. In una cornice di questo tipo non sono contenuti elementi speciali del messaggio.

Lo scambio iniziale tra l'AP e il WLC (interfaccia ap-manager) è di circa 6.000 byte e una modifica alla configurazione una tantum è di circa 360 byte e interessa 2 pacchetti ciascuno dall'AP e

dall'interfaccia ap-manager del WLC.

## Gestione risorse radio (RRM)

Figura 5: Flusso di pacchetti RRM iniziale

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

Una volta eseguito il provisioning dell'access point, viene effettuato uno scambio di informazioni relativo all'RRM. Uno scambio tipico tra l'AP e il WLC (interfaccia ap-manager) è di circa 1400 byte. In caso di modifica della configurazione relativa a RRM, viene effettuato uno scambio di quattro pacchetti tra l'AP e l'interfaccia ap-manager del WLC. Questo scambio ha una media di 375 byte.

Un'acquisizione di esempio di 20 minuti che include l'individuazione, il join, la configurazione e i processi in corso ha generato queste statistiche sul traffico su un segmento di 100 Mbps:

Tabella 1. Statistiche iniziali del traffico LWAPP per un singolo access point

Statistica	Valore
Byte totali	84,869
Utilizzo medio (percentuale)	0.001
Utilizzo medio (kilobit/s)	0.425
Utilizzo massimo (percentuale)	0.004
Utilizzo massimo (kilobit/s)	5.384

La Figura 6 è una rappresentazione grafica dell'intero processo.

Figura 6: Confronto dei protocolli durante la fase di individuazione, aggiunta e provisioning dell'access point

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

## Scambi in corso

### Heartbeat

L'architettura LWAPP fornisce un timer heartbeat che viene realizzato da una serie di **richieste e risposte echo**. Un access point invia periodicamente richieste echo per determinare lo stato della connessione tra l'access point e il WLC. In risposta, il WLC invia la risposta echo per confermare la ricezione della richiesta echo. L'access point reimposta quindi il timer di heartbeat su **EchoInterval**. La bozza delle specifiche del protocollo LWAPP contiene una descrizione dettagliata di questi timer. L'heartbeat di sistema, insieme al meccanismo di fallback, è di 4 pacchetti ogni 30 secondi ed è composto da questi pacchetti:

```
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)
```

Questo scambio genera 33 byte di traffico ogni 30 secondi.

### Misurazioni RRM

Sono in corso due scambi RRM. Il primo, ogni 60 secondi, misura il carico e il segnale ed è composto da 4 pacchetti. Questo scambio aggiunge sempre fino a 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)
```

La seconda sequenza di pacchetti è la misurazione del rumore che include una richiesta di informazioni statistiche e una sequenza di risposta. Viene eseguito ogni 180 secondi. Questo breve scambio di pacchetti dura in media circa 2.660 byte e generalmente 0,01 secondi. È costituito dai seguenti pacchetti:

```
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

### Misurazioni anomale

Le misurazioni non autorizzate vengono effettuate come parte del meccanismo di scansione e incluse nello scambio RRM ogni 180 secondi. Per ulteriori informazioni, fare riferimento a [Gestione risorse radio in Reti wireless unificate](#).

L'acquisizione di esempio di 20 minuti ha prodotto i seguenti valori per gli scambi di pacchetti su un segmento di 100 Mbps:

**Tabella 2. Statistiche del traffico LWAPP in corso per un singolo access point**

Statistica	Valore
Byte totali	45,805
Utilizzo medio (percentuale)	< 0,001
Utilizzo medio (kilobit/s)	0.35
Utilizzo massimo (percentuale)	< 0,001
Utilizzo massimo (kilobit/s)	0.002

Le statistiche e gli scambi riportati nella tabella 2 sono illustrati nelle seguenti immagini:

**Figura 7: Esempio di confronto tra protocolli della durata di 20 minuti mentre l'access point è in funzionamento normale**

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

**Figura 8: Confronto tra i valori dei byte del traffico dei dati LWAPP e il controllo LWAPP**

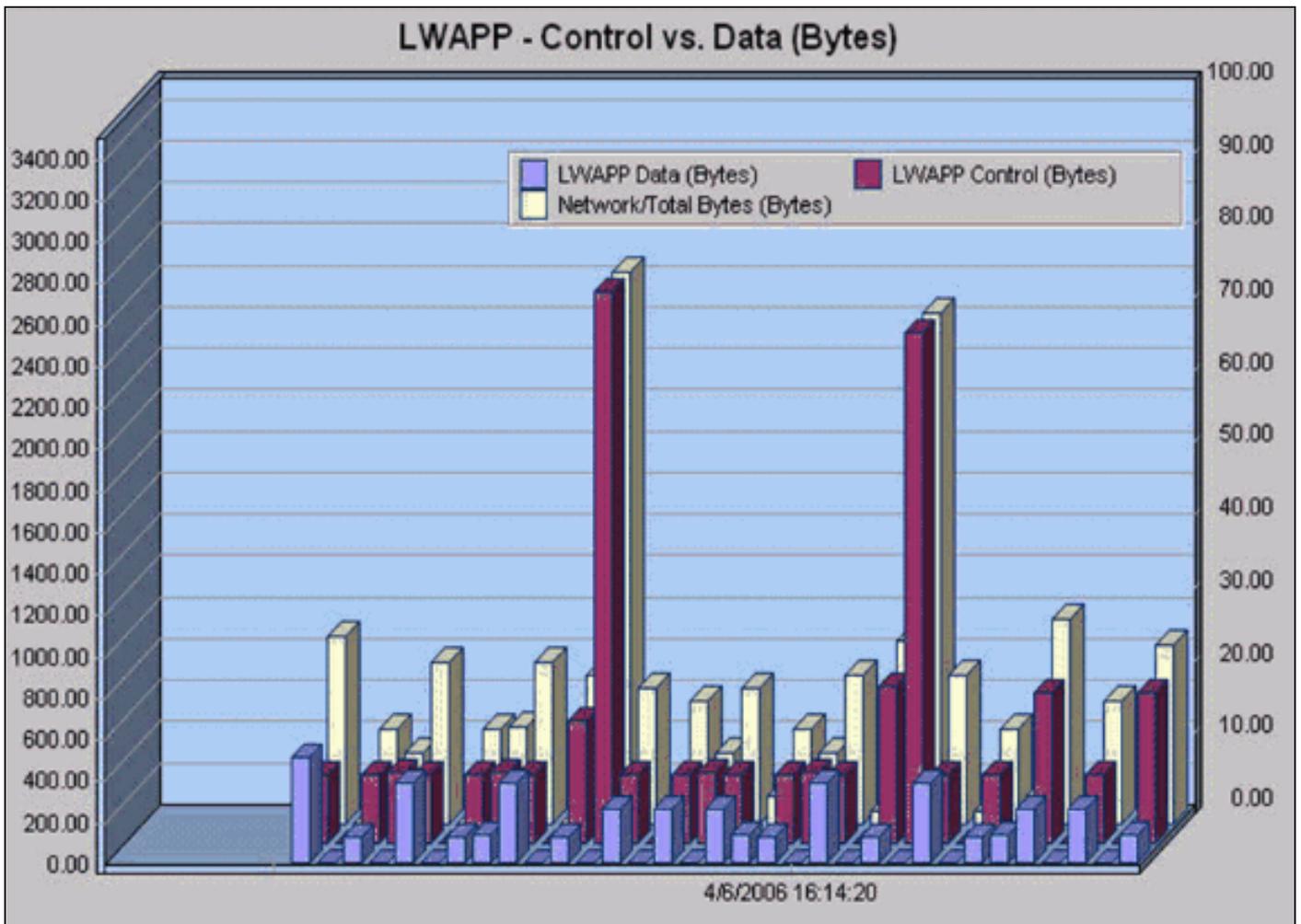
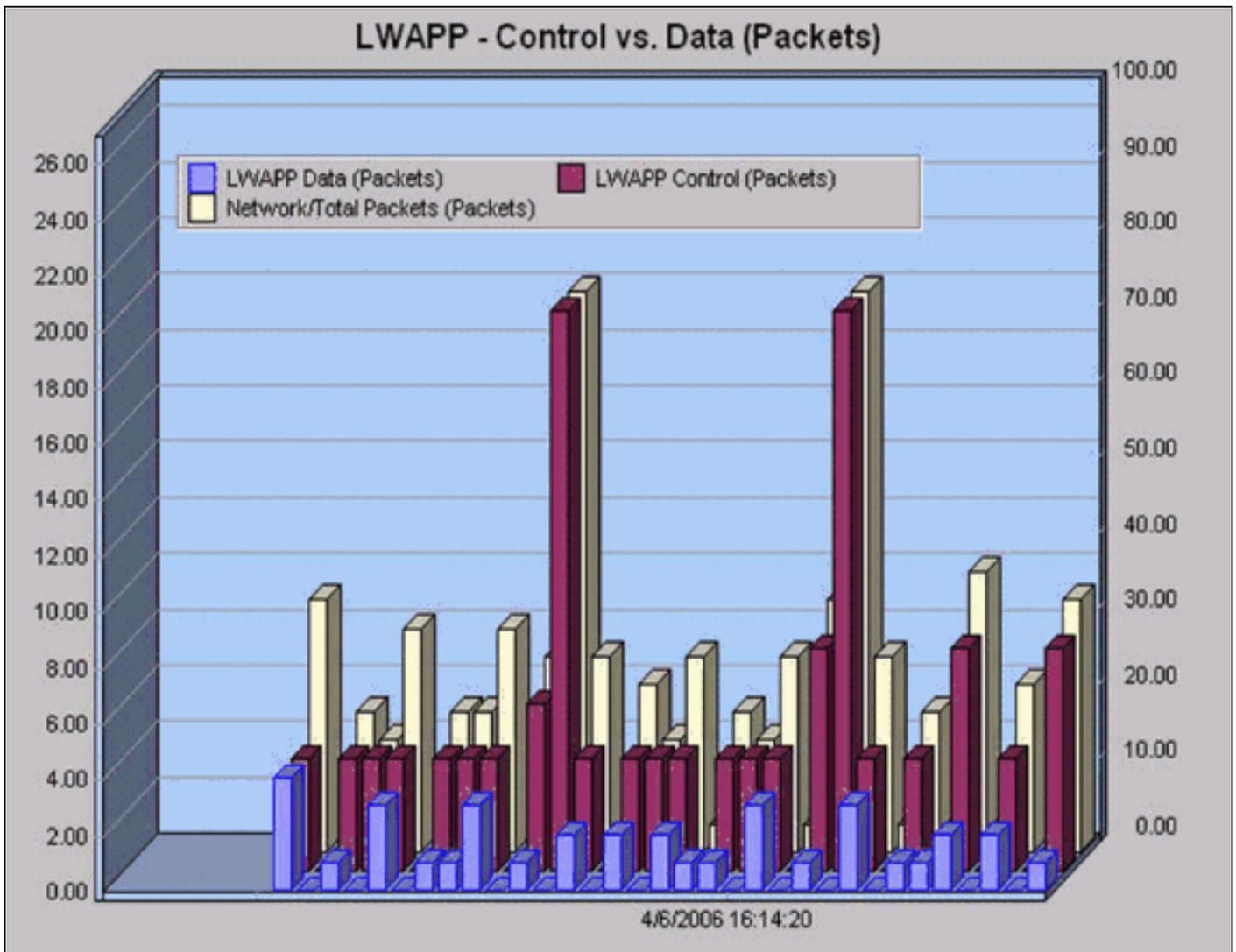


Figura 9: Confronto tra controllo LWAPP e conteggi pacchetti traffico dati LWAPP



## Dati LWAPP

### Spaziatura interna frame

L'intestazione del frame dati LWAPP aggiunge 6 byte ai pacchetti 802.11 esistenti. Questa intestazione viene aggiunta prima del frame 802.11 incapsulato e include quanto segue:

```

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]
  
```

### Frammentazione

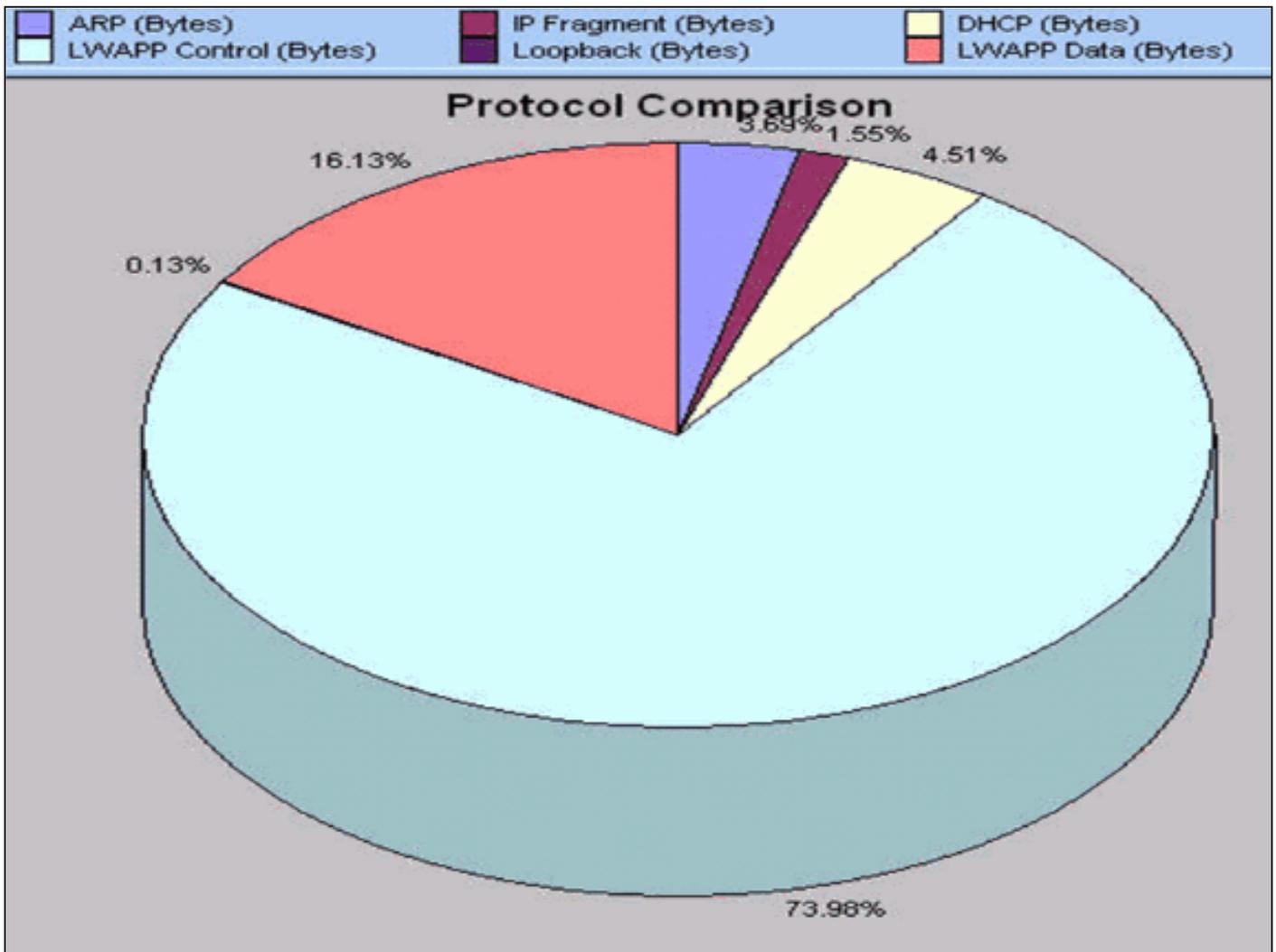
Poiché i frame LWAPP possono essere frammentati, è incluso un campo ID frammento. Le dimensioni totali del pacchetto possono essere determinate aggiungendo il frame originale e il frammento IP. È importante notare che il frammento IP non è incapsulato in alcuna intestazione LWAPP.

## Conclusioni

Come evidenziato dai risultati di questo studio sul traffico, il funzionamento di LWAPP non introduce requisiti di larghezza di banda elevati sull'infrastruttura e, nella maggior parte delle implementazioni tipiche, non è necessario aggiungere ulteriore capacità all'infrastruttura per supportare l'architettura wireless unificata di Cisco. Come riepilogo dello studio sul traffico, si possono tenere a mente questi rapidi fatti sul funzionamento di LWAPP:

- Sebbene la latenza sia un fattore importante, questo studio sul traffico presenta solo considerazioni sulla velocità di trasmissione. Come regola generale, il collegamento AP-WLC non deve superare la latenza di andata e ritorno di 100 ms.
- Esistono due canali distinti per il funzionamento di LWAPP: Dati LWAPP e Traffico LWAPP Control
- Il funzionamento di LWAPP è suddiviso in due grandi categorie: scambi occasionali e scambi in corso
- Un campione di 20 minuti che include gli scambi iniziali genera una statistica di utilizzo medio dello 0,001%.
- Un campione di 20 minuti di scambi in corso genera una statistica di utilizzo massimo di 0,35 kilobit/secondo.
- Il canale dati LWAPP aggiunge un'intestazione di 6 byte a ciascun pacchetto dati 802.11. Non vi è alcun sovraccarico aggiuntivo per i frammenti IP.
- Un esempio di un'ora presenta questa suddivisione dei protocolli e le rispettive percentuali:

**Figura 10: Confronto tra i protocolli basati su un'acquisizione di 1 ora con traffico di dati ridotto, frammenti IP e LWAPP di maggioranza**



## Informazioni correlate

- [Registrazione di un Lightweight AP \(LAP\) su un Wireless LAN Controller \(WLC\)](#)
- [Nozioni fondamentali di LWAPP](#)
- [Ripristino della configurazione di LWAPP su un Lightweight AP \(LAP\)](#)
- [Suggerimenti per la risoluzione dei problemi relativi allo strumento di aggiornamento LWAPP](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)