Étude du trafic LWAPP

Contenu

Introduction

Le projet IETF-RFC, soumis au groupe de travail CAPWAP (Control And Provisioning of Wireless Access Points), décrit le protocole LWAPP (Light Weight Access Point Protocol) comme un protocole développé dans le but de définir des directives de communication entre les points de terminaison sans fil (Access Points) et les contrôleurs d'accès (Wireless LAN Controllers). Toutes les communications LWAPP peuvent être classées dans l'un des deux types de message suivants :

- Canal de contrôle LWAPP
- Données encapsulées LWAPP

LWAPP peut fonctionner en mode de transport de couche 2 ou de couche 3. Les communications LWAPP de couche 2 sont encapsulées dans des trames Ethernet et peuvent être identifiées avec une valeur EtherType de 0x88BB. En raison de sa fiabilité sur Ethernet, le mode de fonctionnement LWAPP de couche 2 n'est pas routable et nécessite une visibilité de couche 2 entre les WLC et les AP. La couche 2 est considérée comme obsolète et les statistiques de protocole présentées dans cette étude du trafic sont basées sur le mode de transport LWAPP de couche 3. Le mode de transport LWAPP de couche 3 spécifie l'échange de messages LWAPP sur le réseau IP sous forme de paquets encapsulés UDP. Le tunnel LWAPP est maintenu avec l'adresse IP de l'interface WLC (gestionnaire d'ap) et l'adresse IP de l'AP. Cette étude du trafic révèle le volume réel de surcharge que les messages LWAPP présentent sur un réseau et une ligne de base du fonctionnement LWAPP dans une installation standard.

Note : La spécification LWAPP est traitée en détail dans la version préliminaire LWAPP-IETF.

Configuration

Ce document présente des statistiques relatives au fonctionnement du protocole LWAPP uniquement et toute fonctionnalité qui n'est pas définie par la spécification du protocole, telle que

l'itinérance inter-contrôleur, n'entre pas dans le champ d'application de ce document. En outre, l'étude du trafic couvre uniquement le mode de fonctionnement LWAPP de couche 3.

Figure 1 : Configuration de l'étude du trafic LWAPP

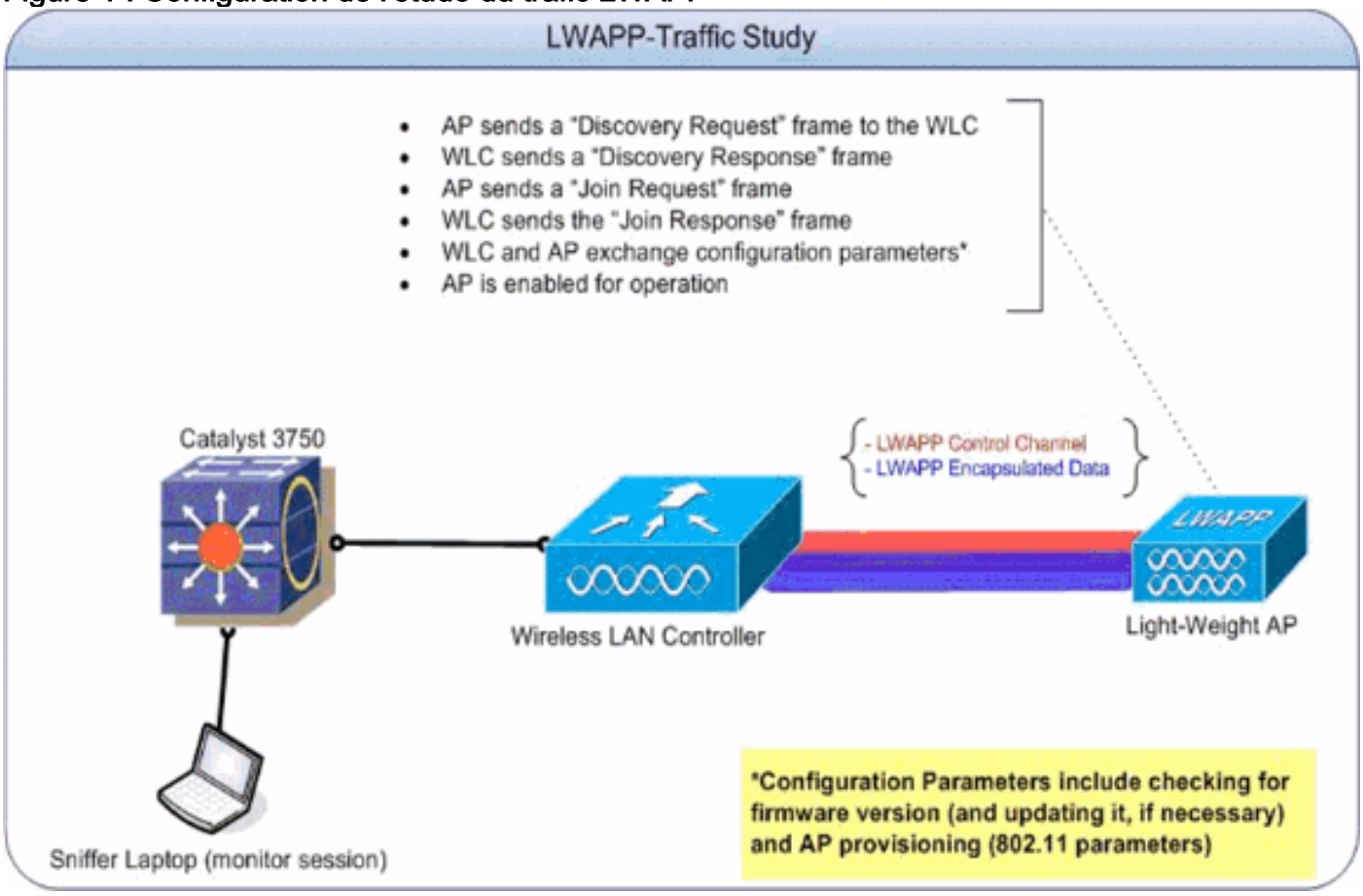


Tableau 1 : Adresses IP de référence pour les périphériques impliqués dans l'étude de trafic LWAPP

Interface/Périphérique	Adresse IP
WLC - Interface de gestion	192.168.10.102
WLC - interface ap-manager	192.168.10.103
Point d'accès léger	192.168.10.22

Aux fins de cette étude du trafic, la configuration a été créée avec un seul point d'accès pour établir les lignes de base de l'échange initial et des modifications de configuration. Plus de points d'accès ont été ajoutés ultérieurement pour déterminer les effets de l'évolution du nombre de points d'accès sur la quantité de trafic générée sur le câble.

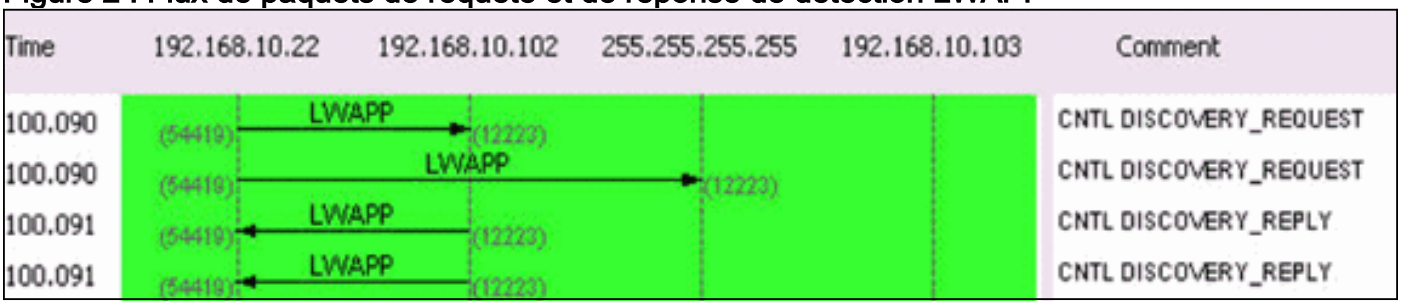
Canal de contrôle LWAPP

Le point d'accès utilise des ports éphémères lorsqu'il communique avec le WLC. Les numéros de port utilisés par le WLC, en retour, sont le port UDP 12222 et le port UDP 12223 pour le trafic de données LWAPP et le trafic de contrôle LWAPP respectivement. Une trame de contrôle LWAPP se distingue d'une trame de données LWAPP par le bit " C " dans le champ d'indicateur d'en-tête du LWAPP. Si la valeur est 1, il s'agit d'une trame de contrôle.

Échanges initiaux/uniques

Détection LWAPP (requête et réponse)

Figure 2 : Flux de paquets de requête et de réponse de détection LWAPP

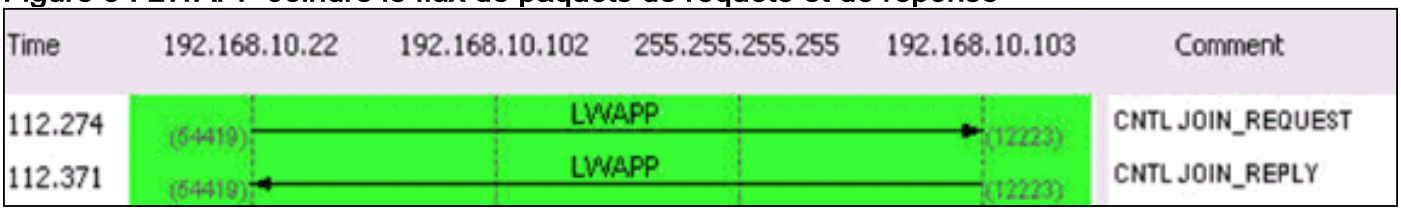


Les requêtes de découverte LWAPP, envoyées par le point d'accès, sont utilisées afin de déterminer quels WLC sont présents dans le réseau.

Un paquet de requête de détection est de 97 octets, ce qui inclut la séquence de contrôle de trame de 4 octets. Un paquet de réponse de détection est de 106 octets, ce qui inclut la séquence de contrôle de trame de 4 octets.

LWAPP Join (Demande et réponse)

Figure 3 : LWAPP Joindre le flux de paquets de requête et de réponse



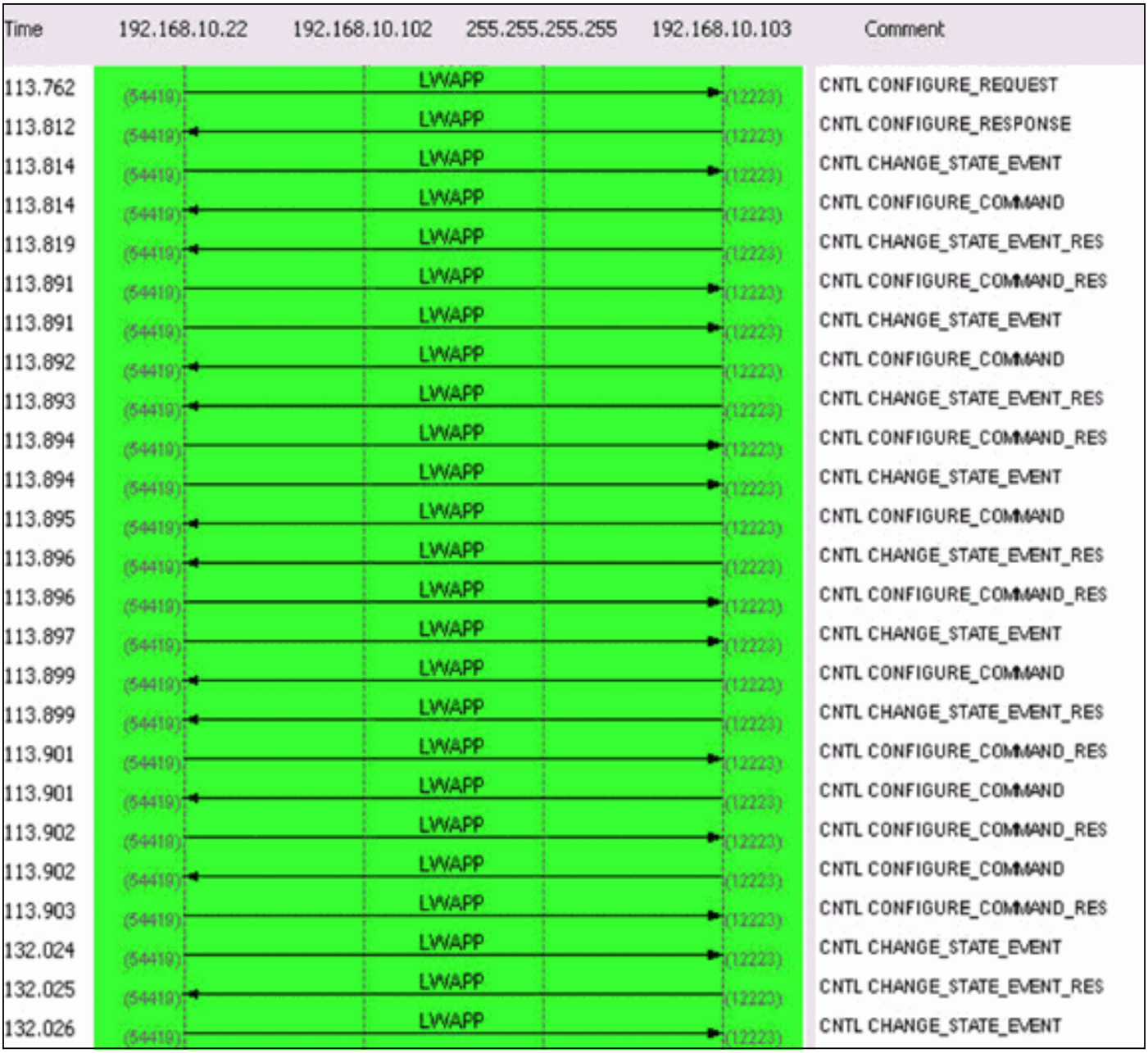
Un paquet de demande de jointure LWAPP est utilisé par le point d'accès afin d'informer le WLC qu'il veut servir les clients par l'intermédiaire du contrôleur. La phase de demande de jointure est également utilisée afin de découvrir le MTU pris en charge par le transport. La demande de jointure initiale envoyée par le point d'accès est toujours complétée par un élément de test de 1 596 octets. En fonction de la façon dont le transport entre l'AP et le contrôleur est configuré, ces trames de demande de jointure peuvent également être fragmentées. Si une réponse de jointure est reçue pour la demande initiale, le point d'accès transfère les trames sans fragmentation. La réponse de jointure initie également le compteur de pulsation (une valeur de 30 secondes) qui, lorsqu'il expire, supprime la session WLC-AP. Le compteur est actualisé à la réception de la demande d'écho ou des accusés de réception.

Si la demande de jointure initiale ne donne aucune réponse, le point d'accès envoie une autre demande de jointure avec l'élément de test, ce qui porte la charge utile totale à 1500 octets. Si la deuxième demande de jointure ne donne pas de réponse non plus, l'AP continue à faire le cycle entre les paquets volumineux et petits et finit par expirer pour recommencer à partir de la phase de découverte.

La taille des paquets pour les messages de demande de jointure et de réponse varie en fonction de la description, mais l'échange de paquets capturé aux fins de cette étude de trafic entre l'AP et le WLC (interface ap-manager) est de 3 000 octets.

Configuration LWAPP

Figure 4 : LWAPP Configurer le flux de paquets d'état et de mise en service des points d'accès



Les requêtes et réponses de configuration LWAPP sont échangées entre les points d'accès et les contrôleurs afin de créer, modifier (mettre à jour) ou supprimer les services offerts par un point d'accès.

En général, un message Configure Request est envoyé par un point d'accès pour envoyer sa configuration actuelle à son WLC.

La demande de configuration peut être envoyée dans deux scénarios :

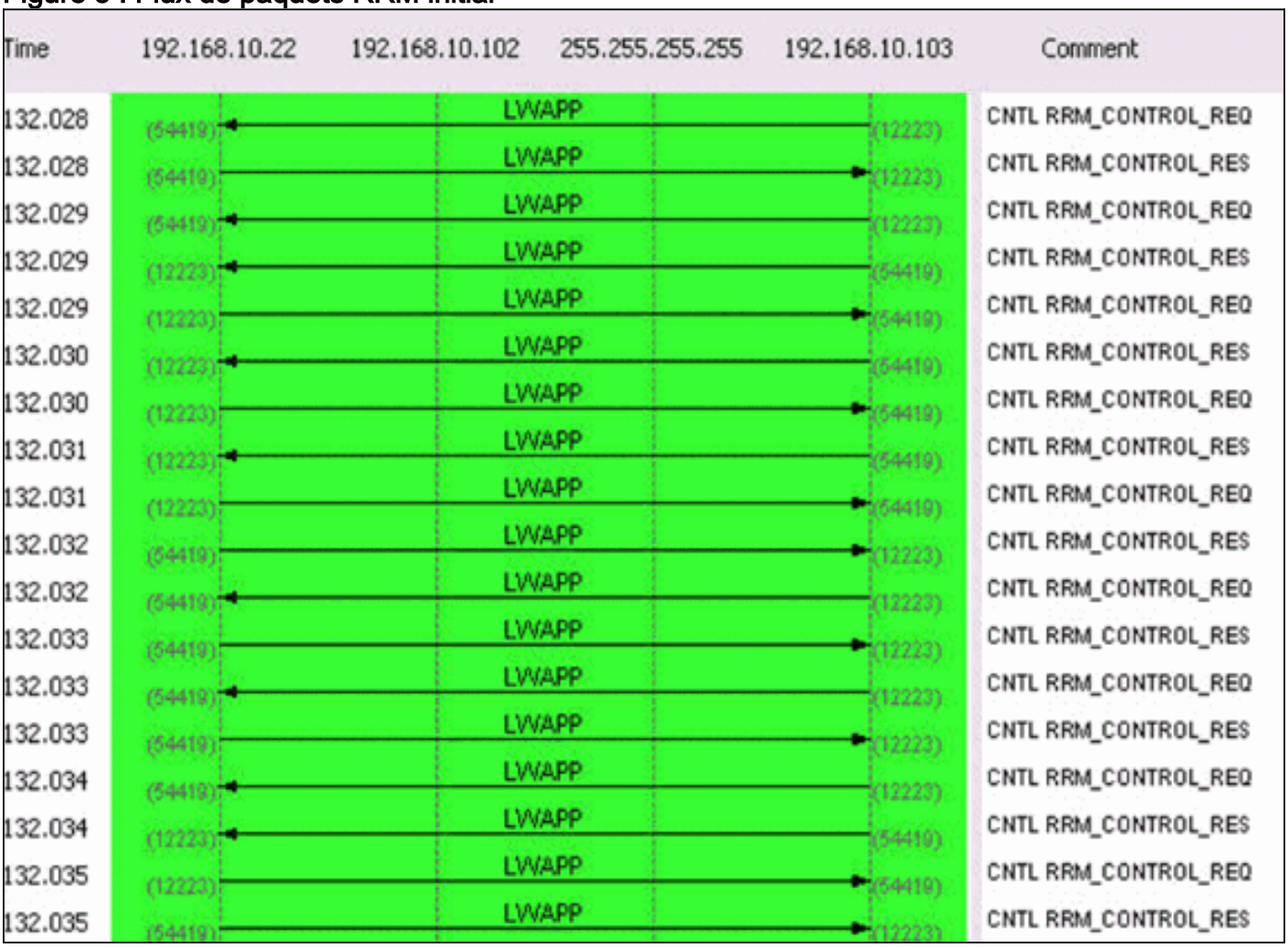
1. Dans la phase initiale, lorsque l'AP rejoint un contrôleur et doit être provisionné avec tous les paramètres 802.11 configurés sur le contrôleur.
2. Dans le cas de modifications administratives à la demande, telles qu'une modification d'un paramètre WLAN

Le type de message de réponse de configuration LWAPP est envoyé par le WLC au point d'accès afin d'accuser réception de la demande de configuration LWAPP de la part du point d'accès. Ceci fournit une opportunité pour le WLC de remplacer la configuration demandée par l'AP. Il n'y a aucun élément de message spécial contenu dans une telle trame.

L'échange initial entre l'AP et le WLC (interface ap-manager) est d'environ 6 000 octets et un changement de configuration unique est en moyenne de 360 octets et implique 2 paquets chacun de l'AP et de l'interface ap-manager du WLC.

[Gestion des ressources radio (RRM)]

Figure 5 : Flux de paquets RRM initial



Un échange d'informations relatives à RRM a lieu une fois que le point d'accès est provisionné. Un échange typique entre l'AP et le WLC (interface ap-manager) est d'environ 1 400 octets. En cas de changement de configuration lié à RRM, il y a un échange de quatre paquets entre l'AP et l'interface gestionnaire d'ap du WLC. Cet échange fait en moyenne 375 octets.

Une capture d'échantillon de 20 minutes comprenant les processus de découverte, de jointure, de configuration et en cours a abouti à ces statistiques de trafic sur un segment de 100 Mbits/s :

Tableau 1 : Statistiques de trafic LWAPP initiales pour un point d'accès unique

Statistique	Valeur
Nombre total d'octets	84,869
Utilisation moyenne (pourcentage)	0.001
Utilisation moyenne (kilobits/s)	0.425
Utilisation maximale (pourcentage)	0.004
Utilisation maximale (kilobits/s)	5.384

La figure 6 représente l'ensemble du processus.

Figure 6 : Comparaison des protocoles lors de la phase de découverte, de jointure et de mise en service des points d'accès

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

Échanges en cours

Tête de coeur

L'architecture LWAPP fournit un compteur de pulsation qui est réalisé par une série de **requêtes Echo** et de **réponses Echo**. Un point d'accès envoie périodiquement des requêtes d'écho afin de déterminer l'état de la connexion entre le point d'accès et le WLC. En réponse, le WLC envoie la réponse d'écho afin d'accuser réception de la demande d'écho. Le point d'accès réinitialise alors le compteur de pulsation sur l'**EchoInterval**. Le projet de spécification de protocole LWAPP contient une description détaillée de ces temporisateurs. La pulsation système, associée à un mécanisme de secours, est de 4 paquets toutes les 30 secondes et comprend les paquets suivants :

```
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)
```

Cet échange génère 33 octets de trafic toutes les 30 secondes.

Mesures RRM

Deux échanges de MRR sont en cours. La première, à chaque intervalle de 60 secondes, est la mesure de la charge et du signal et se compose de 4 paquets. Cet échange totalise toujours 396 octets :

```
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 deuxième séquence de paquets est la mesure du bruit qui inclut une requête d'informations statistiques et une séquence de réponses. Il est effectué toutes les 180 secondes. Cet échange court de paquets dure en moyenne environ 2 660 octets et dure généralement 0,01 seconde. Il se compose des paquets suivants :

```
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
```

Mesures non fiables

Les mesures non fiables sont effectuées dans le cadre du mécanisme de balayage et incluses dans l'échange RRM toutes les 180 secondes. Référez-vous à Gestion des ressources radio sous Réseaux sans fil unifiés pour plus d'informations.

La capture d'échantillons de 20 minutes a donné les valeurs suivantes pour les échanges de paquets en cours sur un segment de 100 Mbits/s :

Tableau 2 : Statistiques de trafic LWAPP continues pour un point d'accès unique

Statistique	Valeur
Nombre total d'octets	45,805
Utilisation moyenne (pourcentage)	< 0,001
Utilisation moyenne (kilobits/s)	0,35
Utilisation maximale (pourcentage)	< 0,001
Utilisation maximale (kilobits/s)	0.002

Les statistiques et les échanges du tableau 2 sont illustrés dans ces images :

Figure 7 : Un échantillon de comparaison de protocole de 20 minutes pendant que le point d'accès fonctionne normalement

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

Figure 8 : Contrôle LWAPP par rapport aux valeurs d'octets de trafic de données LWAPP

comparées

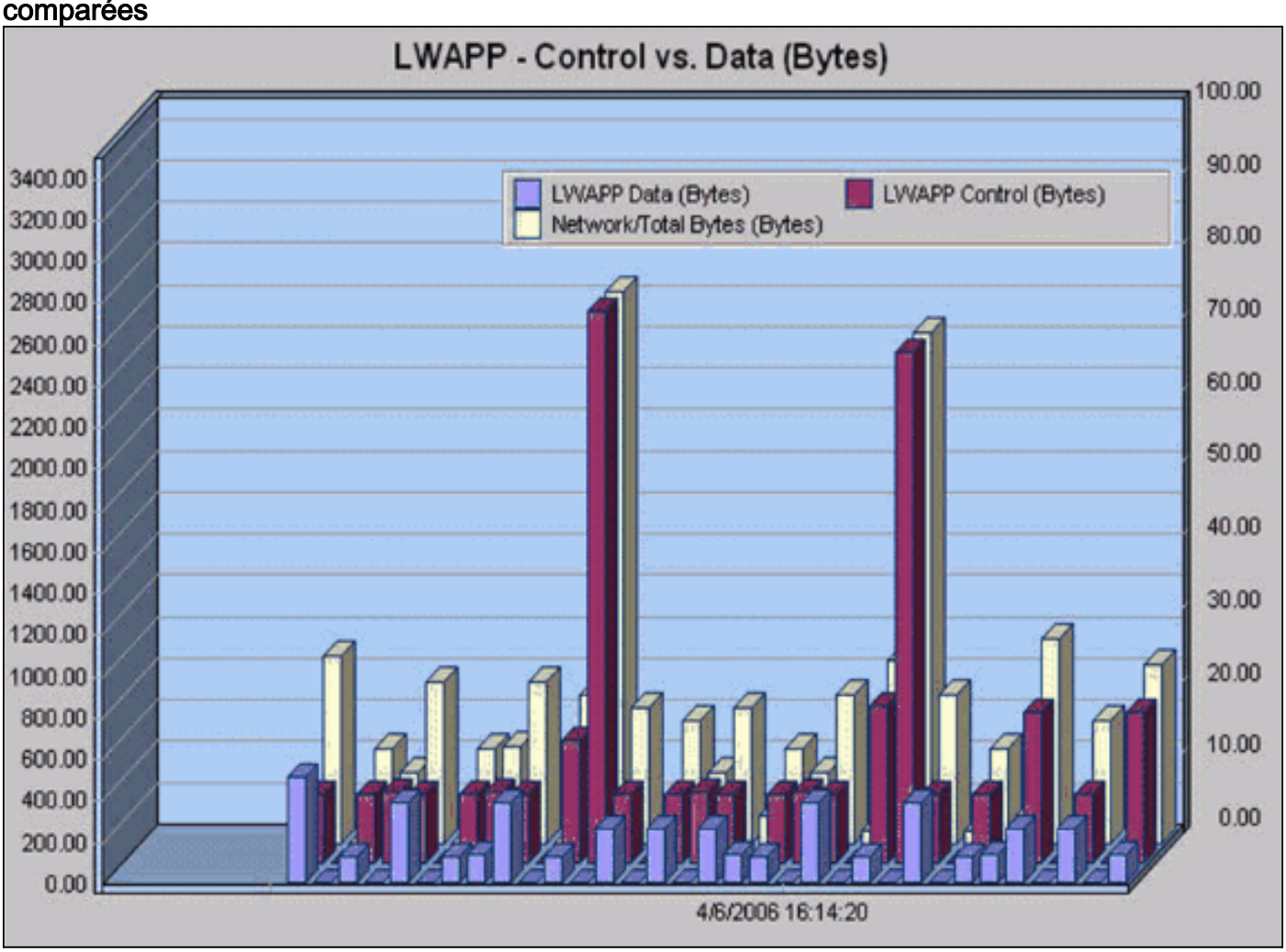
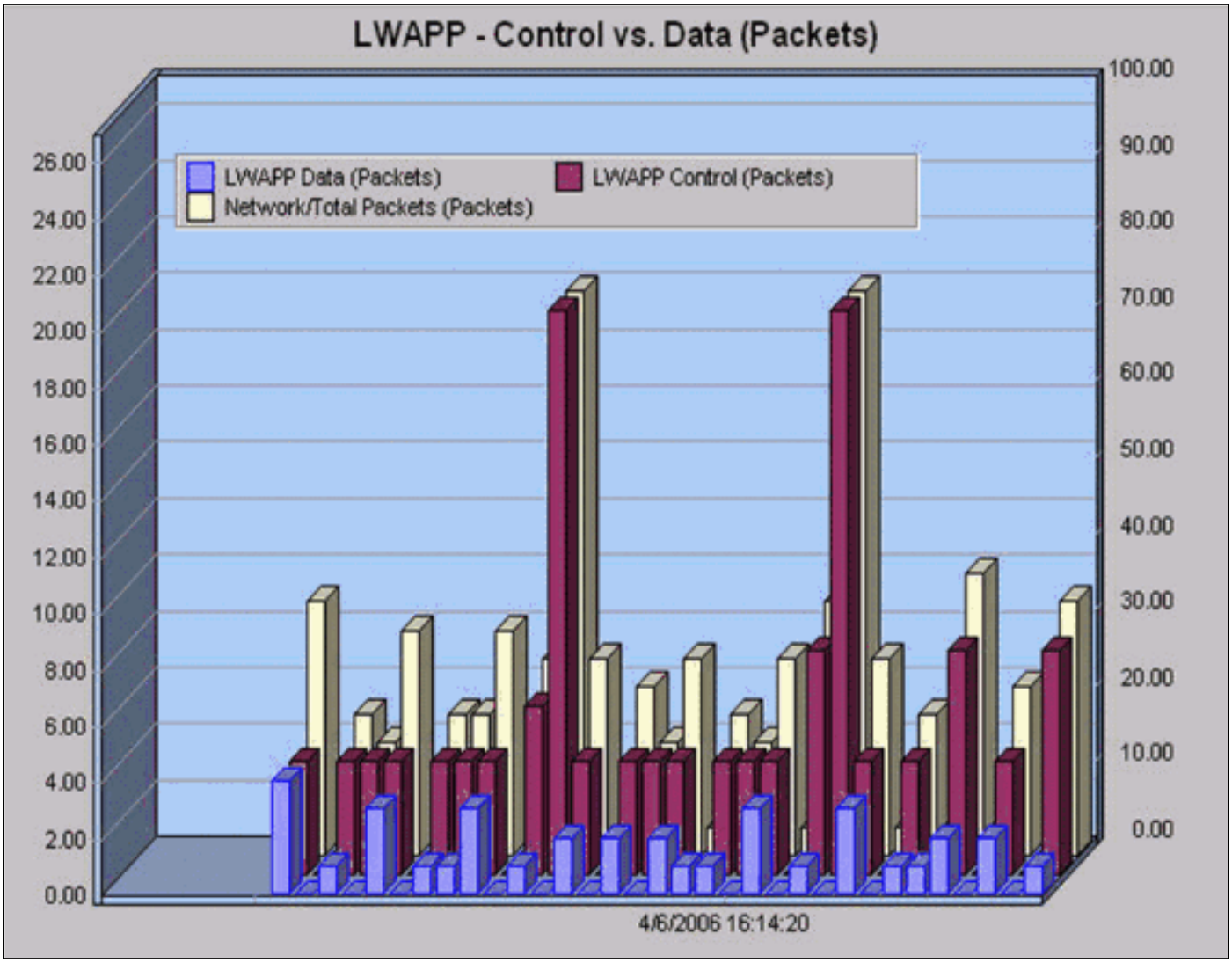


Figure 9 : Comparaison du nombre de paquets de trafic de données LWAPP et du contrôle LWAPP



Données LWAPP

Remplissage de trame

L'en-tête de trame de données LWAPP ajoute 6 octets aux paquets 802.11 existants. Cet en-tête est ajouté avant la trame 802.11 encapsulée et comprend les éléments suivants :

```
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]
```

Fragmentation

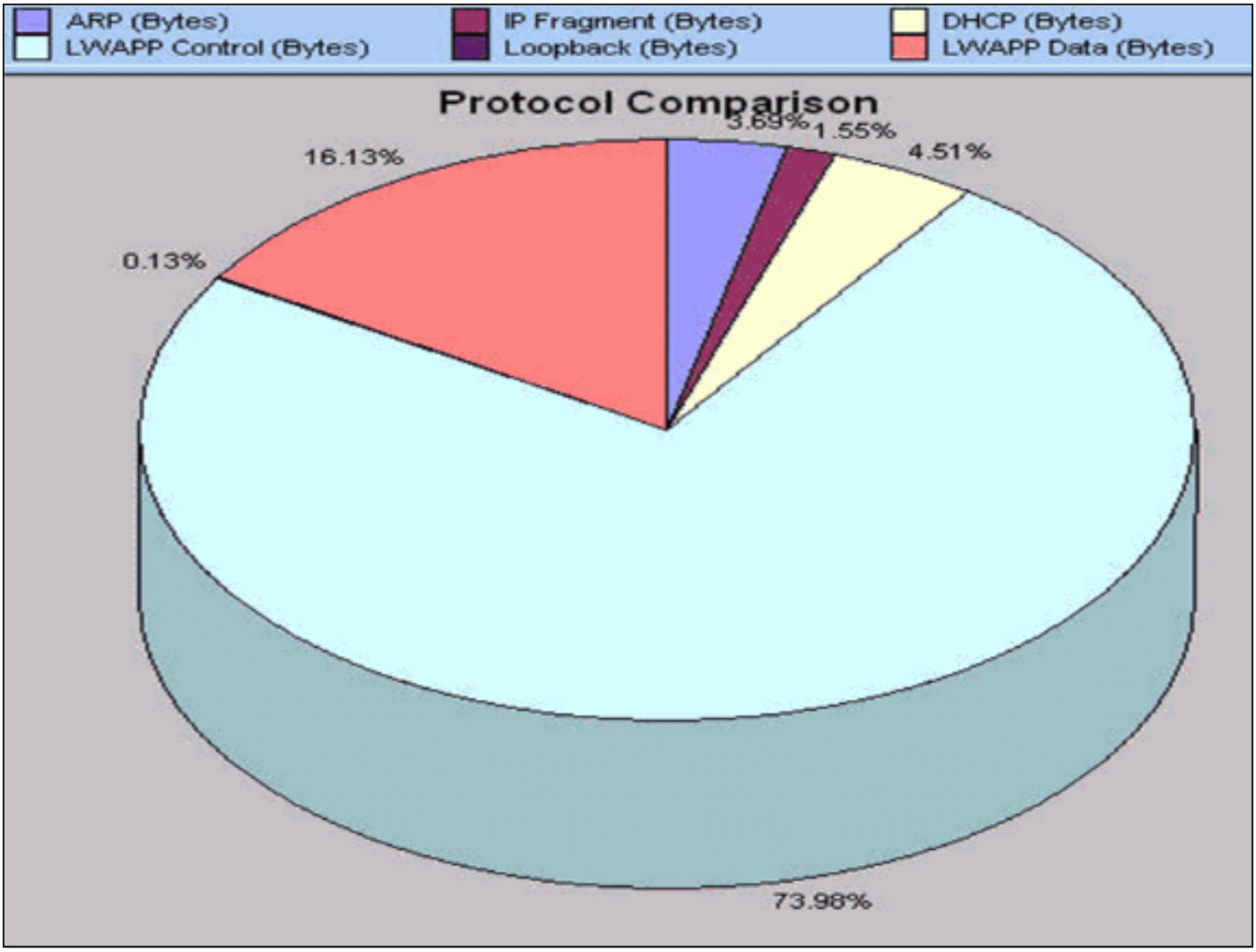
Comme les trames LWAPP peuvent être fragmentées, un champ ID de fragment est inclus. La taille totale du paquet peut être déterminée si vous ajoutez la trame d'origine et le fragment IP. Il est important de noter que le fragment IP n'est encapsulé dans aucun en-tête LWAPP.

Conclusion

Comme le montrent les résultats de cette étude sur le trafic, le fonctionnement du LWAPP n'introduit pas de besoins importants en bande passante sur l'infrastructure et, dans la plupart des déploiements standard, il n'est pas nécessaire d'ajouter une capacité supplémentaire à l'infrastructure afin de prendre en charge l'architecture sans fil unifiée de Cisco. Pour résumer l'étude sur le trafic, il est possible de garder à l'esprit ces faits rapides sur le fonctionnement du LWAPP :

- Bien que la latence soit une considération importante, cette étude du trafic ne présente que des considérations de débit. En règle générale, la liaison AP-WLC ne doit pas dépasser 100 ms de latence aller-retour.
- Il existe deux canaux distincts pour le fonctionnement du LWAPP :Données LWAPPTrafic de contrôle LWAPP
- L'opération LWAPP est divisée en deux grandes catégories :échanges uniqueséchanges continus
- Un échantillon de 20 minutes qui inclut les échanges initiaux donne un taux d'utilisation moyen de 0,001 %.
- Un échantillon de 20 minutes d'échanges en cours donne une statistique d'utilisation maximale de 0,35 kilobits/seconde.
- Le canal de données LWAPP ajoute un en-tête de 6 octets à chaque paquet de données 802.11. Il n'y a pas de surcharge supplémentaire pour les fragments IP.
- Un échantillon d'une heure présente cette ventilation des protocoles et leurs pourcentages respectifs :

Figure 10 : Comparaison de protocoles basée sur une capture d'une heure avec trafic de données faible, fragments IP et LWAPP majoritaire



Informations connexes

- Enregistrement d'un point d'accès léger (LAP) sur un contrôleur LAN sans fil (WLC)
- Notions de base LWAPP
- Réinitialisation de la configuration LWAPP sur AP léger (LAP)
- Conseils de dépannage de l'outil de mise à niveau LWAPP
- Support et documentation techniques - Cisco Systems