Étude du trafic LWAPP

Contenu

Introduction

L'ébauche IETF-RFC, soumise au contrôle et au ravitaillement du groupe de travail des points d'accès sans fil (CAPWAP), décrit le point d'accès léger Protocol (LWAPP) comme protocole développé avec le but pour définir des instructions de transmission entre les points d'arrêt Sans fil (Points d'accès) et pour accéder à des contrôleurs (contrôleurs LAN Sans fil). Toutes les transmissions LWAPP peuvent être classifiées dans un de ces deux types de message :

- Canal de contrôle LWAPP
- Données encapsulées par LWAPP

LWAPP peut fonctionner mode dans de la couche 2 ou de la couche 3 transport. Des transmissions de la couche 2 LWAPP sont encapsulées dans des trames Ethernet et peuvent être identifiées avec une valeur Ethertype de 0x88BB. En raison de son sérieux sur des Ethernets, posez le mode de fonctionnement 2 LWAPP n'est pas routable et exige la visibilité de la couche 2 entre le WLCs et les aps. La couche 2 est considérée désapprouvée et des statistiques de protocole tracées les grandes lignes dans cette étude du trafic sont basées sur le mode de transport de la couche 3 LWAPP. Le mode de transport de la couche 3 LWAPP spécifie l'échange des messages LWAPP sur le réseau IP sous forme de paquets UDP-encapsulés. Le tunnel LWAPP est mis à jour avec l'adresse IP de l'interface WLC (AP-gestionnaire) et l'adresse IP d'AP. Cette étude du trafic indique le montant effectif de temps système que les messages LWAPP actuels sur un réseau et une spécification de base d'exécution LWAPP dans une norme installent.

Remarque: La spécification LWAPP est discutée en détail à l'[ébauche LWAPP-IETF](#).

Installation

Ce document présente des statistiques liées à l'exécution de LWAPP seulement et n'importe quelle fonctionnalité qui n'est pas définie par la spécification de protocole, telle que l'itinérance d'inter-contrôleur, est hors de portée de ce document. En outre, les couvertures d'étude du trafic

seulement posent le mode 3 de l'exécution LWAPP.

Figure 1 : Installation d'étude du trafic LWAPP

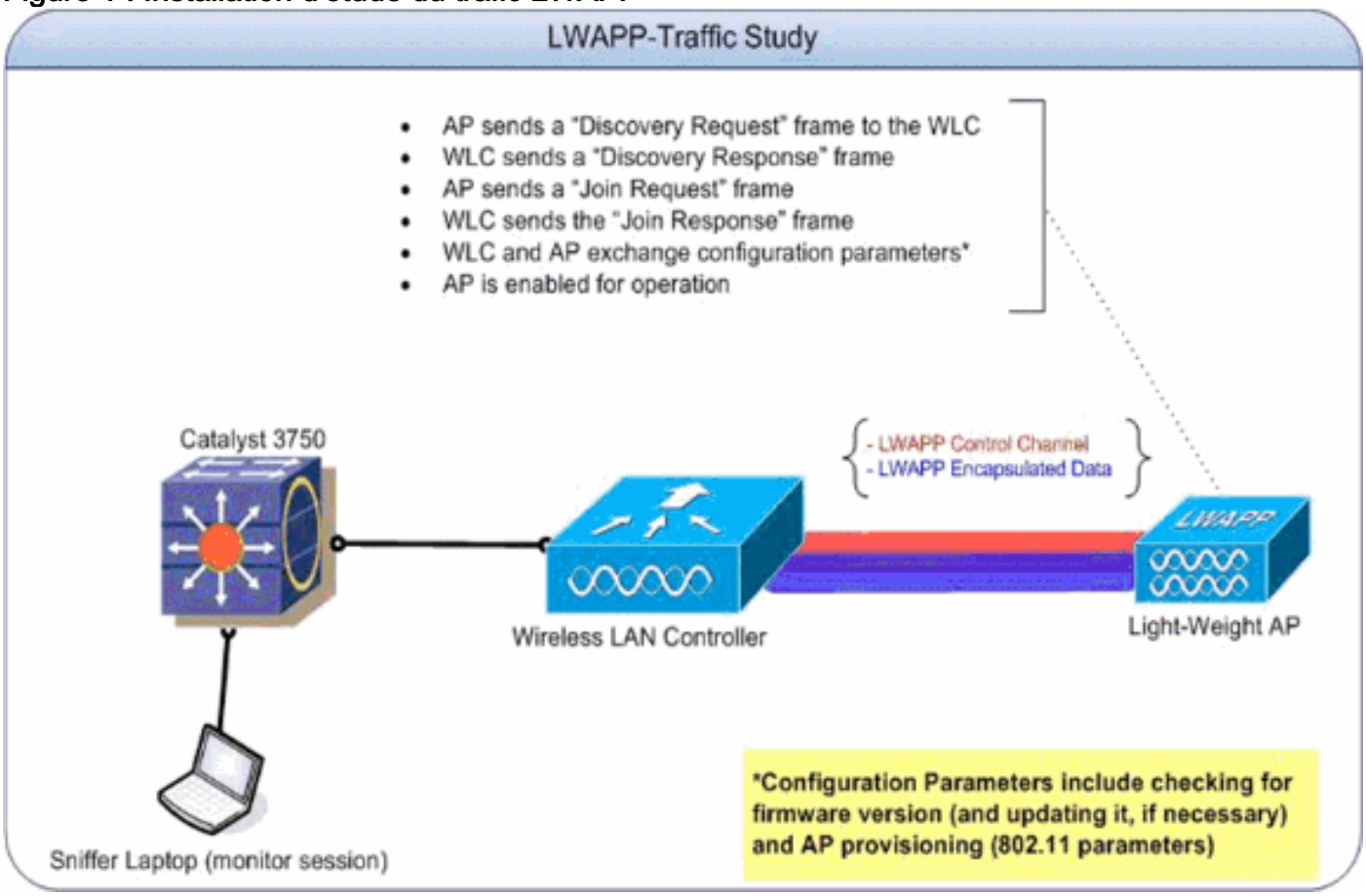


Tableau 1 : Adresses IP référentielles pour des périphériques impliqués dans la trafic-étude LWAPP

Interface/périphérique	Adresse IP
WLC - Interface de gestion	192.168.10.102
WLC - interface d'AP-gestionnaire	192.168.10.103
AP léger	192.168.10.22

Aux fins de cette étude du trafic, l'installation a été créée avec seulement un Point d'accès pour établir les spécifications de base initiales de modifications d'échange et de configuration. Plus d'aps plus tard ont été ajoutés pour déterminer les effets de mesurer le nombre d'aps sur le niveau de trafic généré sur le fil.

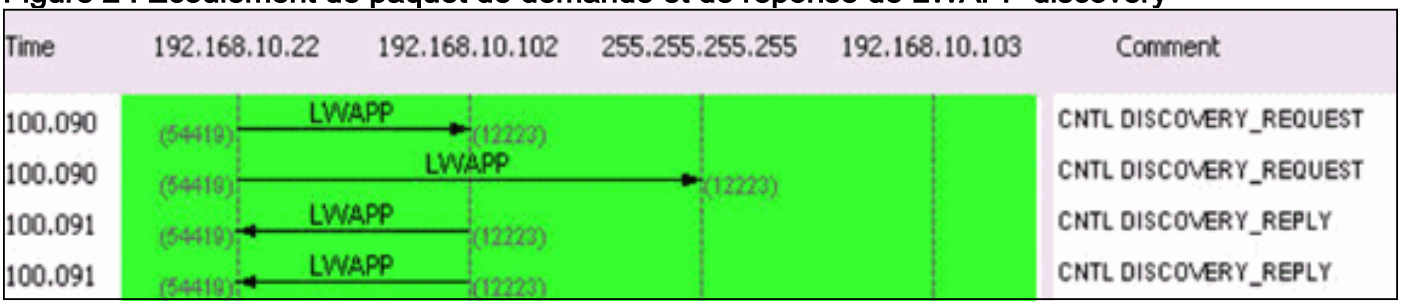
Canal de contrôle LWAPP

AP utilise les ports éphémères quand il parle au WLC. Les numéros de port utilisés par le WLC, en échange, sont le port UDP 12222 et le port UDP 12223 pour le trafic de données LWAPP et de contrôle LWAPP respectivement. Une trame de contrôle LWAPP est distinguée d'une trame de données LWAPP par le « C » mordue dans le champ d'indicateur d'en-tête du LWAPP. Si réglé à 1, c'est une trame de contrôle.

Initiale/échanges une fois

LWAPP discovery (demande et réponse)

Figure 2 : Écoulement de paquet de demande et de réponse de LWAPP discovery

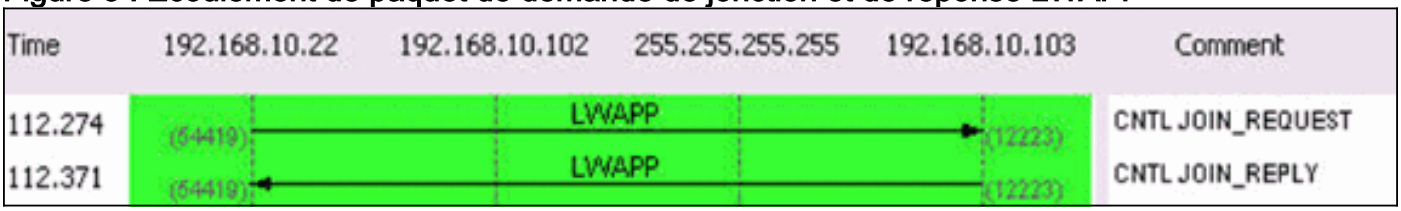


Les demandes de LWAPP discovery, envoyées par le Point d'accès, sont utilisées afin de déterminer quel WLCs sont présent dans le réseau.

Un paquet de demande de détection est de 97 octets, qui inclut la FCS de 4 octets. Un paquet de réponse de détection est de 106 octets, qui inclut la FCS de 4 octets.

LWAPP se joignent (demande et réponse)

Figure 3 : Écoulement de paquet de demande de jonction et de réponse LWAPP



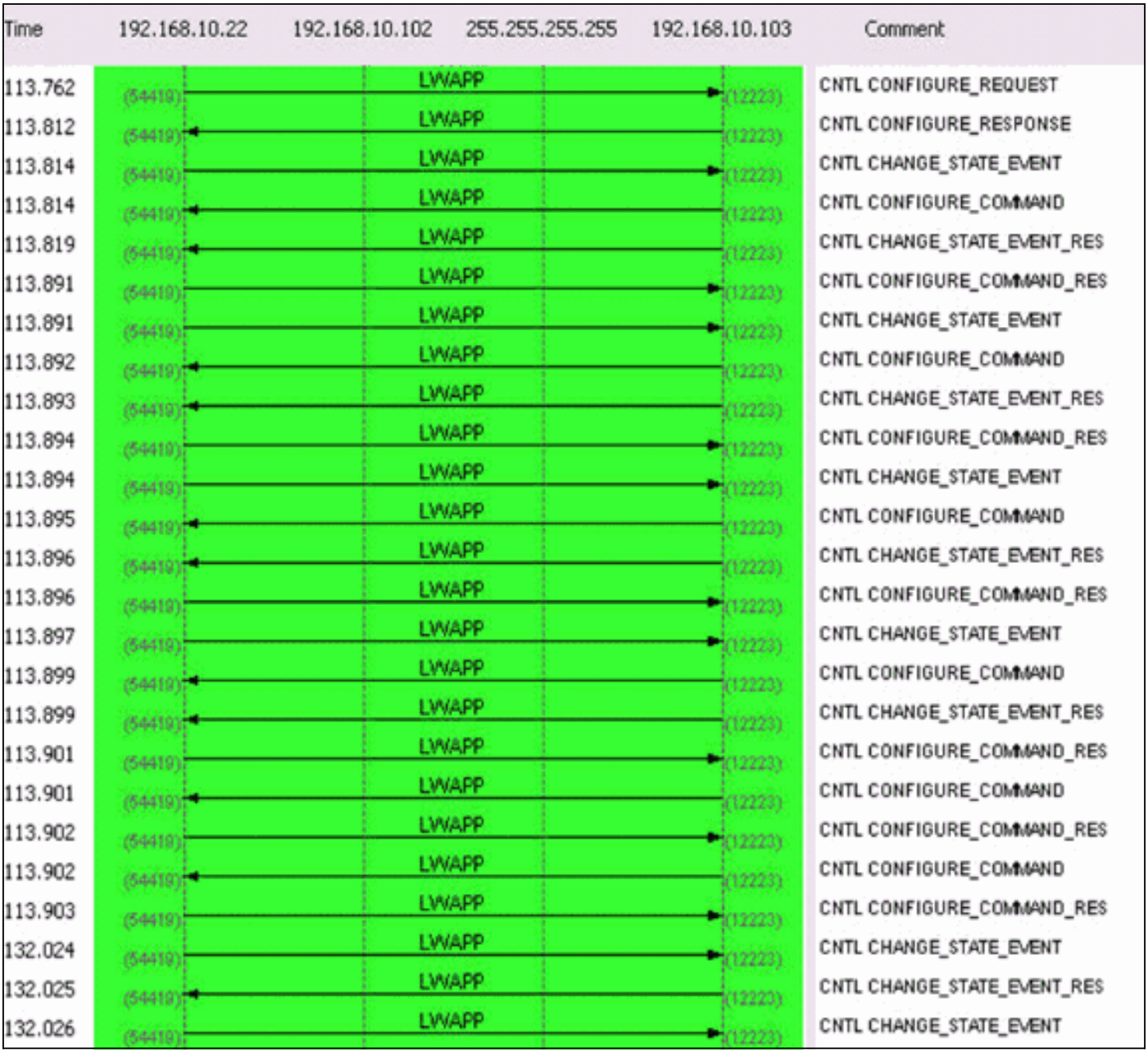
Un paquet de demande de jonction LWAPP est utilisé par le Point d'accès afin d'informer le WLC qu'il veut entretenir des clients par le contrôleur. La phase de demande de jonction est également utilisée afin de découvrir le MTU pris en charge en le transport. La demande de jonction initiale envoyée par le Point d'accès est toujours complétée avec un élément de test de 1596 octets. Basé sur la façon dont le transport entre AP et le contrôleur est installé, ces trames de demande de jonction peuvent être aussi bien fragmentées. Si une réponse de jonction est reçue pour la requête initiale, AP les trames en avant sans toute fragmentation. La réponse de jonction initie également le temporisateur de pulsation (une valeur 30-second) qui, quand il expire, supprime la session WLC-AP. Le temporisateur est régénéré sur la réception de la requête d'écho ou des accusés de réception.

Si la demande de jonction initiale ne rapporte aucune réponse, AP envoie une autre demande de jonction avec l'élément de test, qui apporte toute la charge utile à 1500 octets. Si la deuxième demande de jonction ne rapporte pas une réponse non plus, AP continue à faire un cycle entre les grands et petits paquets et chronomètre par la suite pour recommencer de la phase de détection.

Les longueurs de paquet pour les messages de demande de jonction et de réponse varient basé sur la description mais l'échange de paquet capturé aux fins de cette trafic-étude entre AP et le WLC (interface d'AP-gestionnaire) est de 3,000 octets.

Config LWAPP

Figure 4 : LWAPP configurent l'écoulement de paquet d'état et de ravitaillement AP



Les demandes et les réponses de config LWAPP sont permutées entre les Points d'accès et les contrôleurs afin de créer, changer (mise à jour) ou supprimer les services offerts par AP.

Généralement un message de demande de configurer est envoyé par AP pour envoyer sa configuration en cours à son WLC.

La demande de config peut être introduite deux scénarios :

1. Pendant la phase initiale où AP joint un contrôleur et doit provisioned avec toutes les configurations de 802.11 qui sont configurées sur le contrôleur.
2. Dans le cas des modifications administratives sur demande, telles qu'une modification à un paramètre WLAN

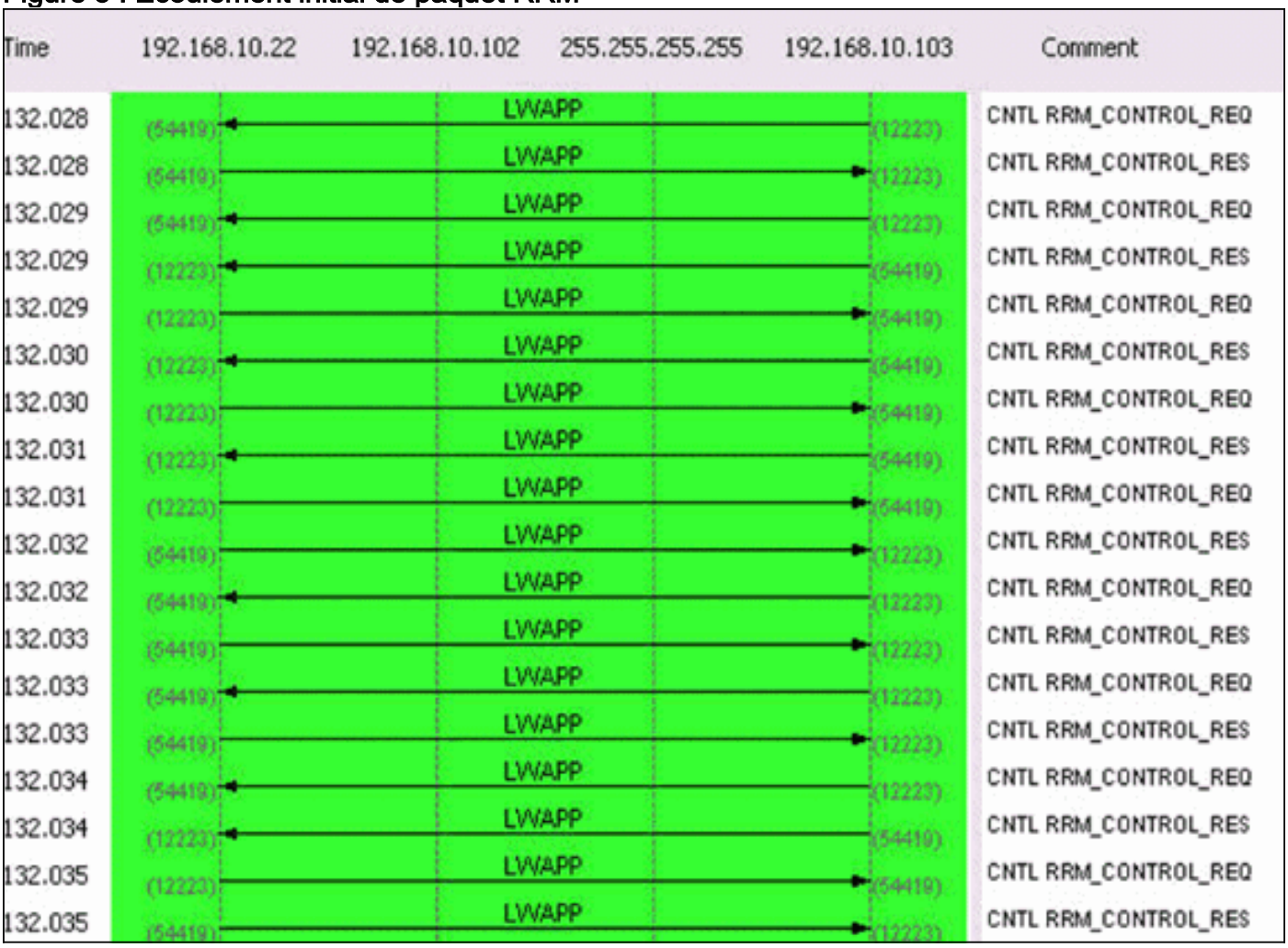
Le type de message de réponse de config LWAPP est envoyé par le WLC à AP afin d'accuser réception de la demande de config LWAPP d'AP. Ceci présente un moyen du WLC d'ignorer la configuration demandée d'AP. Il n'y a aucun élément de message spécial contenu par une telle trame.

L'échange initial entre AP et le WLC (interface d'AP-gestionnaire) est approximativement 6,000

octets et moyennes une fois d'une modification de configuration 360 octets et implique 2 paquets chacun d'AP et l'interface d'AP-gestionnaire du WLC.

[Gestion des ressources radio (RRM)]

Figure 5 : Écoulement initial de paquet RRM



Un échange d'informations lié RRM a lieu une fois qu'AP provisioned. Un échange typique entre AP et le WLC (interface d'AP-gestionnaire) est approximativement 1400 octets. En cas d'une modification de configuration liée RRM, il y a un échange de quatre-paquet entre AP et l'interface d'AP-gestionnaire du WLC. Cet échange fait la moyenne de 375 octets.

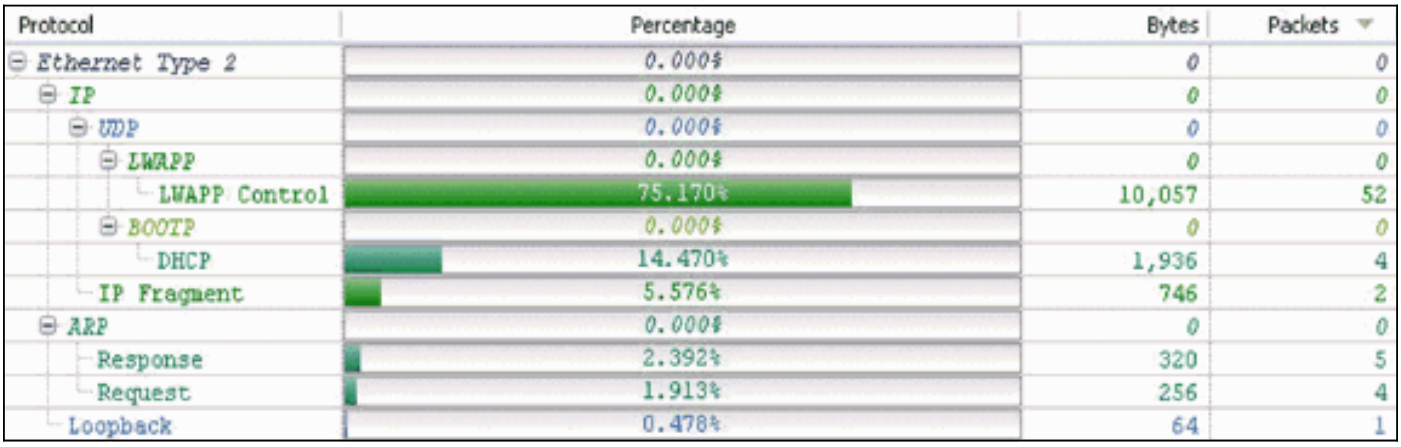
Une capture témoin de 20-minute qui inclut la détection, se joignent, configuration, et les processus actuels ont eu comme conséquence ces statistiques de trafic sur un segment de 100 Mbits/s :

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

Statistique	Valeur
Octets totaux	84,869
Utilisation moyenne (pour cent)	0.001
Utilisation moyenne (kilobits/s)	0.425
Utilisation maximum (pour cent)	0.004
Utilisation maximum (kilobits/s)	5.384

La figure 6 est une représentation imagée du processus entier.

Figure 6 : La comparaison de Protocol pendant la détection AP, se joignent et la phase de ravitaillement



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 actuels

Pulsation

L'architecture LWAPP prévoit un temporisateur de pulsation qui est accompli par une gamme de **requêtes d'écho** et de **réponses d'écho**. AP envoie périodiquement des requêtes d'écho afin de déterminer l'état de la connexion entre AP et le WLC. Dans la réponse, le WLC envoie la réponse d'écho afin d'accuser réception de la requête d'écho. AP, alors, remet à l'état initial le temporisateur de pulsation à l'**EchoInterval**. L'ébauche de spécification de protocole LWAPP contient une description détaillée de ces temporisateurs. La pulsation de système, ajoutée au mécanisme de repli, est 4 paquets toutes les 30 secondes et est composée de ces paquets :

```
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 du trafic toutes les 30 secondes.

Mesures RRM

Il y a deux échanges actuels RRM. Le premier, à chaque 60-deuxième intervalle, est la mesure de chargement et de signal et se compose de 4 paquets. Cet échange ajoute toujours à 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)
```

Le deuxième ordre des paquets est la mesure de bruit qui inclut un ordre de demande et de réponse de l'information de statistiques. Il est fait toutes les 180 secondes. Cet échange court des paquets fait la moyenne d'approximativement 2,660 octets et dure typiquement 0.01 seconde. Il se compose de ces paquets :

```
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 escrocs

Des mesures escrocs sont faites comme une partie du mécanisme de balayage et incluses dans l'échange RRM toutes les 180 secondes. Référez-vous à la gestion des ressources par radio sous le pour en savoir plus de réseaux sans fil unifié.

La capture témoin de 20-minute a eu comme conséquence les valeurs suivantes pour des échanges actuels de paquet sur un segment de 100 Mbits/s :

Tableau 2 : Statistiques de trafic actuelles LWAPP pour un seul point d'accès

Statistique	Valeur
Octets totaux	45,805
Utilisation moyenne (pour cent)	< 0.001
Utilisation moyenne (kilobits/s)	0.35
Utilisation maximum (pour cent)	< 0.001
Utilisation maximum (kilobits/s)	0.002

Les statistiques et les échanges dans le tableau 2 sont dépeints dans ces images :

Figure 7 : Un échantillon de 20-minute de comparaison de protocole tandis qu'AP est en fonctionnement le fonctionnement normal

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 contre des valeurs d'octet du trafic de données LWAPP comparées

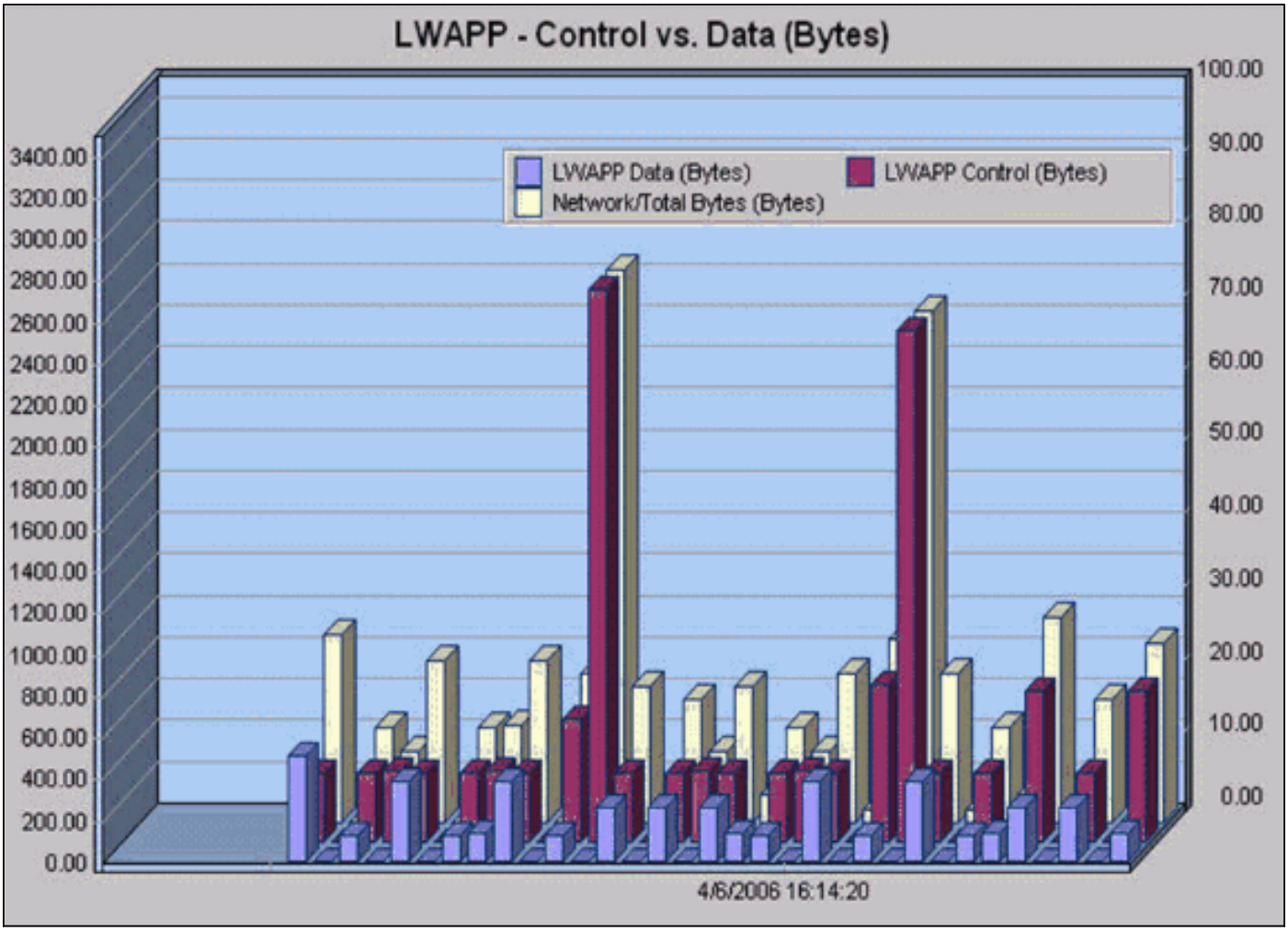
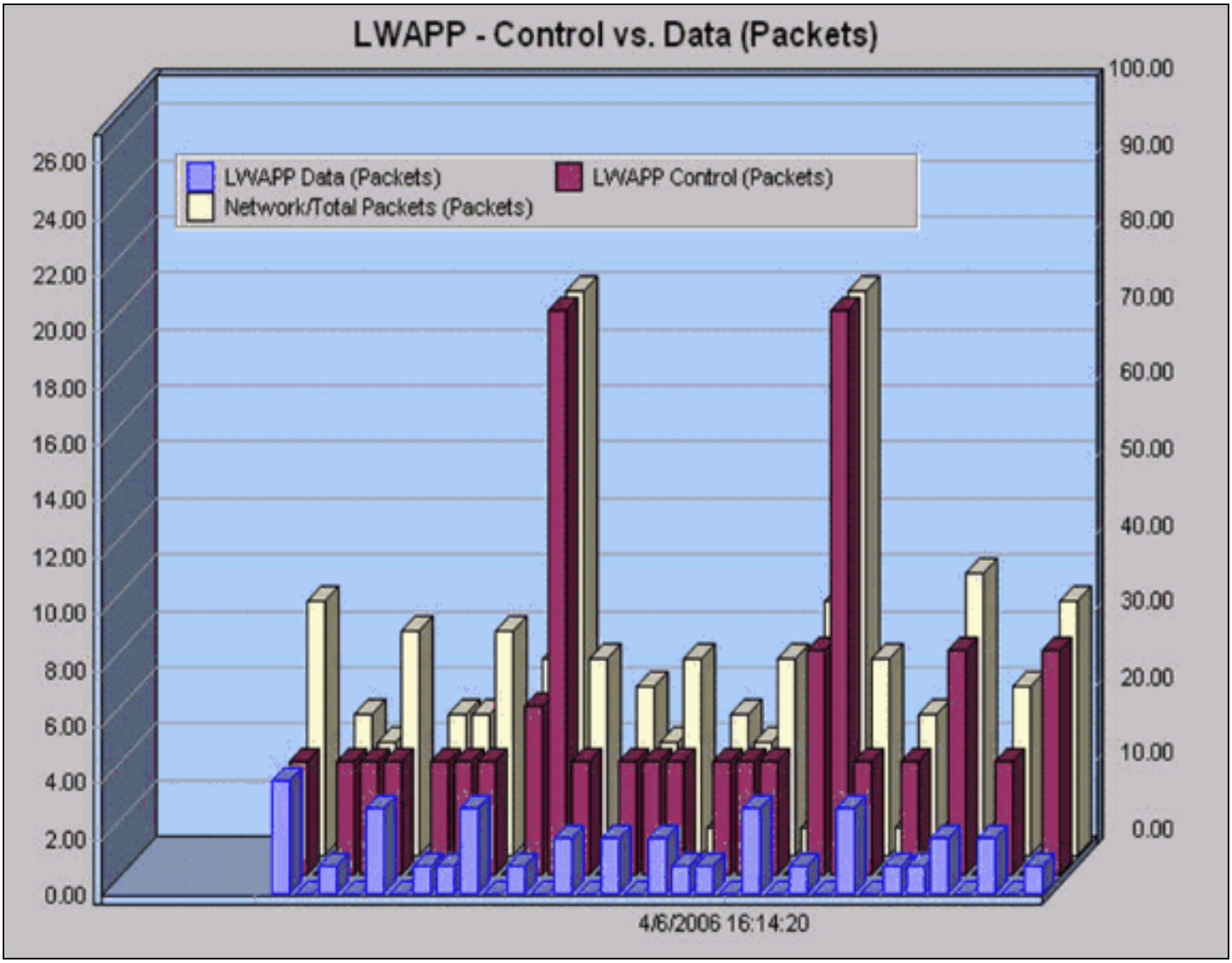


Figure 9 : Contrôle LWAPP contre des comptes de paquet du trafic de données LWAPP comparés



Données LWAPP

Remplissage de trame

L'en-tête de trame de données LWAPP ajoute 6 octets aux paquets existants de 802.11. Cette en-tête est ajoutée avant que la trame encapsulée de 802.11 et inclue ce qui suit :

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

Puisque des trames LWAPP peuvent être fragmentées, un champ d'ID de fragment est inclus. Toute la longueur de 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 aucune en-tête LWAPP.

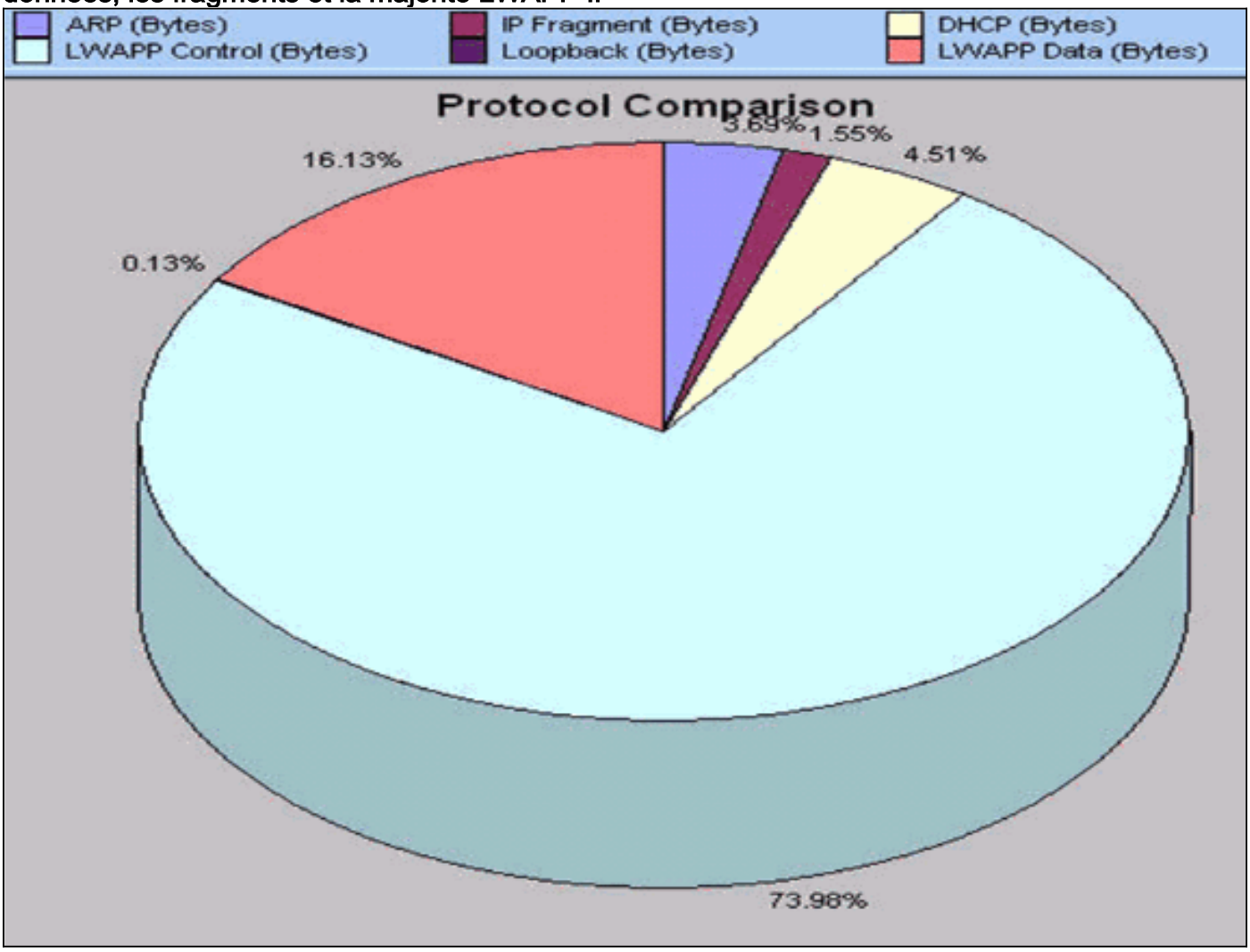
Conclusion

Comme évident par les résultats dans cette étude du trafic, l'exécution de LWAPP n'introduit pas des bandes passantes nécessaires lourdes sur l'infrastructure, et dans la plupart des

déploiements typiques, il n'y a aucun besoin d'ajouter la capacité supplémentaire à l'infrastructure afin de faciliter l'architecture de Cisco Unified Wireless. Comme un résumé de l'étude du trafic, ces faits rapides sur l'exécution de LWAPP peut être maintenu dans l'esprit :

- Bien que la latence soit une importante considération, des considérations de ce de trafic-étude débit de présents seulement. Comme recommandation générale, AP--WLC au lien ne doit pas dépasser la latence 100ms aller-retour.
- Il y a deux canaux distincts pour l'exécution de LWAPP :Données LWAPPLe trafic de contrôle LWAPP
- L'exécution LWAPP est décomposée en deux larges catégories :échanges une foiséchanges actuels
- Un échantillon de 20 minutes qui inclut des échanges initiaux a comme conséquence une statistique moyenne d'utilisation de 0.001 pour cent.
- Un échantillon de 20 minutes d'échanges actuels a comme conséquence une statistique d'utilisation maximale de 0.35 kilobit/seconde.
- La voie de transmission de données LWAPP ajoute une en-tête de 6 octets à chaque paquet de données de 802.11. Il n'y a aucun temps système supplémentaire pour des fragments IP.
- Un échantillon d'une heure présente cette dissolution des protocoles et de leurs pourcentages respectifs :

Figure 10 : Comparaison de Protocol basée sur une capture d'une heure avec le bas trafic de données, les fragments et la majorité LWAPP IP



Informations connexes

- Enregistrement d'un point d'accès léger (LAP) sur un contrôleur LAN sans fil (WLC)
- Principes fondamentaux 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