Configuration des captures de paquets sur AireOS WLC

Contenu

Introduction

Ce document décrit comment exécuter un vidage de paquets sur un contrôleur LAN sans fil AireOS (WLC). Cette méthode affiche les paquets envoyés et/ou reçus au niveau du CPU du WLC au format hexadécimal, qui sont ensuite traduits en fichier .pcap avec Wireshark.

Il est utile dans les cas où la communication entre un WLC et un serveur RADIUS (Remote Authentication Dial-In User Service), un point d'accès (AP) ou d'autres contrôleurs doit être vérifiée rapidement avec une capture de paquets au niveau du WLC, mais une portée de port est difficile à exécuter.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- L'accès à l'interface de ligne de commande (CLI) au WLC, de préférence SSH, car la sortie est plus rapide que la console.
- PC avec Wireshark installé

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC v8.3
- Wireshark v2 ou version ultérieure

Note : Cette fonctionnalité est disponible depuis AireOS version 4.

Limites

La journalisation des paquets capturera uniquement les paquets du plan de contrôle bidirectionnel (CP) vers le plan de données (DP) dans le WLC. Les paquets qui ne sont pas envoyés du plan de données du WLC vers/depuis le plan de contrôle (c'est-à-dire étrangers au trafic d'ancrage tunnelisé, abandons DP-CP, etc.) ne seront pas capturés.

Voici des exemples de types de trafic en provenance/à destination du WLC traité au niveau du CP :

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RADIUS
- TACACS+
- Messages de mobilité
- Contrôle CAPWAP
- NMSP
- TFTP/FTP/SFTP
- Syslog
- IAPP

Le trafic en provenance et à destination du client est traité dans le plan de données (DP), à l'exception des éléments suivants : Gestion 802.11, 802.1X/EAPOL, ARP, DHCP et authentification Web.

Configuration

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Activer la journalisation des paquets dans WLC

Étape 1. Connectez-vous à l'interface de ligne de commande du WLC.

En raison de la quantité et de la vitesse des journaux que cette fonctionnalité affiche, il est recommandé de se connecter au WLC par SSH et non par console.

Étape 2. Appliquez une liste de contrôle d’accès (ACL) pour limiter le trafic capturé.

Dans l'exemple donné, la capture montre le trafic en provenance et à destination de l'interface de gestion du WLC (adresse IP 172.16.0.34) et du serveur RADIUS (172.16.56.153).

```
> debug packet logging acl ip 1 permit 172.16.0.34 172.16.56.153
> debug packet logging acl ip 2 permit 172.16.56.153 172.16.0.34
```

Astuce : Pour capturer tout le trafic en provenance et à destination du WLC, il est recommandé d'appliquer une liste de contrôle d'accès qui rejette le trafic SSH en provenance et à destination de l'hôte qui a initié la session SSH. Voici les commandes que vous pouvez utiliser pour créer la liste de contrôle d'accès :

>debug packet logging acl ip 1 deny <WLC-IP> <host-IP> tcp 22 any
>debug packet logging acl ip 2 deny <host-IP> <WLC-IP> tcp any 22
>debug packet logging acl ip 3 permit any any

Étape 3. Configurez le format lisible par Wireshark.

```
> debug packet logging format text2pcap
```

Étape 4. Activez la fonction de journalisation des paquets.

Cet exemple montre comment capturer 100 paquets reçus/transmis (il prend en charge 1 à 65535 paquets) :

```
> debug packet logging enable all 100
```

Étape 5. Enregistrez la sortie dans un fichier texte.

Note: Par défaut, il enregistre seulement 25 paquets reçus avec la commande **debug packet logging enable**.

Note: Au lieu de **tout** vous pouvez utiliser **rx** ou **tx** pour capturer uniquement le trafic reçu ou transmis.

Pour plus d'informations sur la configuration de la fonction de journalisation des paquets, consultez ce lien :

Guide de configuration du contrôleur sans fil Cisco, version 8.3, Utilisation de la fonction de débogage

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Utilisez la commande donnée pour vérifier la configuration actuelle de la journalisation des paquets.

```
> show debug packet

Status..................................... rx/tx            !!! This means the capture is
active
Number of packets to display..................... 100
Bytes/packet to display.......................... 0
Packet display format............................ text2pcap
```

```
   Driver ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   IP ACL:
      [1]: permit s=172.16.0.34 d=172.16.56.153 any
      [2]: permit s=172.16.56.153 d=172.16.0.34 any
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-Dot11 ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
```

Reproduire le comportement nécessaire pour générer le trafic.

Une sortie similaire à celle-ci apparaît :

```
rx len=108, encap=unknown, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 5A 69 81 00 00 80 01 78 A7 AC 10 ..E..Zi.....x',.
0020 00 38 AC 10 00 22 03 03 55 B3 00 00 00 00 45 00 .8,.."..U3....E.
0030 00 3E 0B 71 00 00 FE 11 58 C3 AC 10 00 22 AC 10 .>.q..~.XC,..",.
0040 00 38 15 B3 13 88 00 2A 8E DF A8 a1 00 0E 00 0E .8.3...*._(!....
```

```
0050 01 00 00 00 00 22 F1 FC 8B E0 18 24 07 00 C4 00 ....."q|.`.$..D.
0060 F4 00 50 1C BF B5 F9 DF EF 59 F7 15 t.P.?5y_oYw.
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 28 69 82 40 00 80 06 38 D3 AC 10 ..E..(i.@...8S,.
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 40 29 50 10 01 01 52 8A 00 00 @)P...R...
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 28 69 83 40 00 80 06 38 D2 AC 10 ..E..(i.@...8R,.
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 41 59 50 10 01 00 51 5B 00 00 AYP...Q[..
rx len=58, encap=ip, port=2
0000 E0 89 9D 43 EF 40 C8 5B 76 1D AB 51 81 00 09 61 `..Co@H[v.+Q...a
0010 08 00 45 00 00 28 69 84 40 00 80 06 38 D1 AC 10 ..E..(i.@...8Q,.
0020 00 38 AC 10 00 22 F6 3A 00 16 AF 52 FE F5 1F 0C .8,.."v:../R~u..
0030 43 19 50 10 01 05 4F 96 00 00 C.P...O...
```

Supprimer les listes de contrôle d'accès de la journalisation des paquets

Afin de désactiver les filtres appliqués par les listes de contrôle d'accès, utilisez ces commandes :

```
> debug packet logging acl ip 1 disable
>debug packet logging acl ip 2 disable
```

Désactiver la journalisation des paquets

Afin de désactiver la journalisation des paquets sans supprimer les listes de contrôle d'accès, utilisez simplement cette commande :

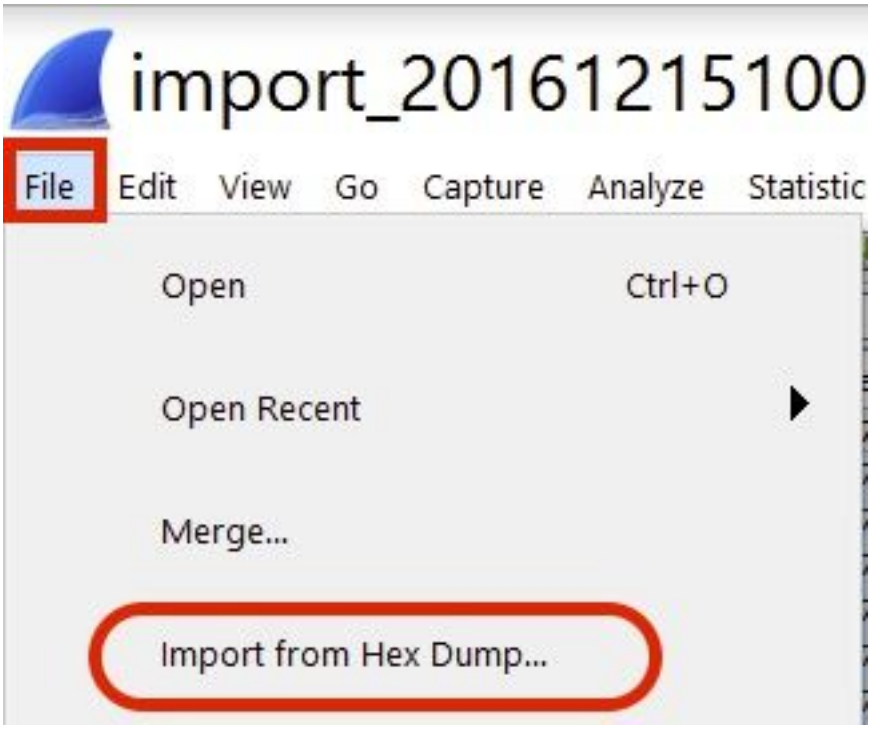
```
> debug packet logging disable
```

Convertir la sortie de journalisation des paquets en fichier .pcap

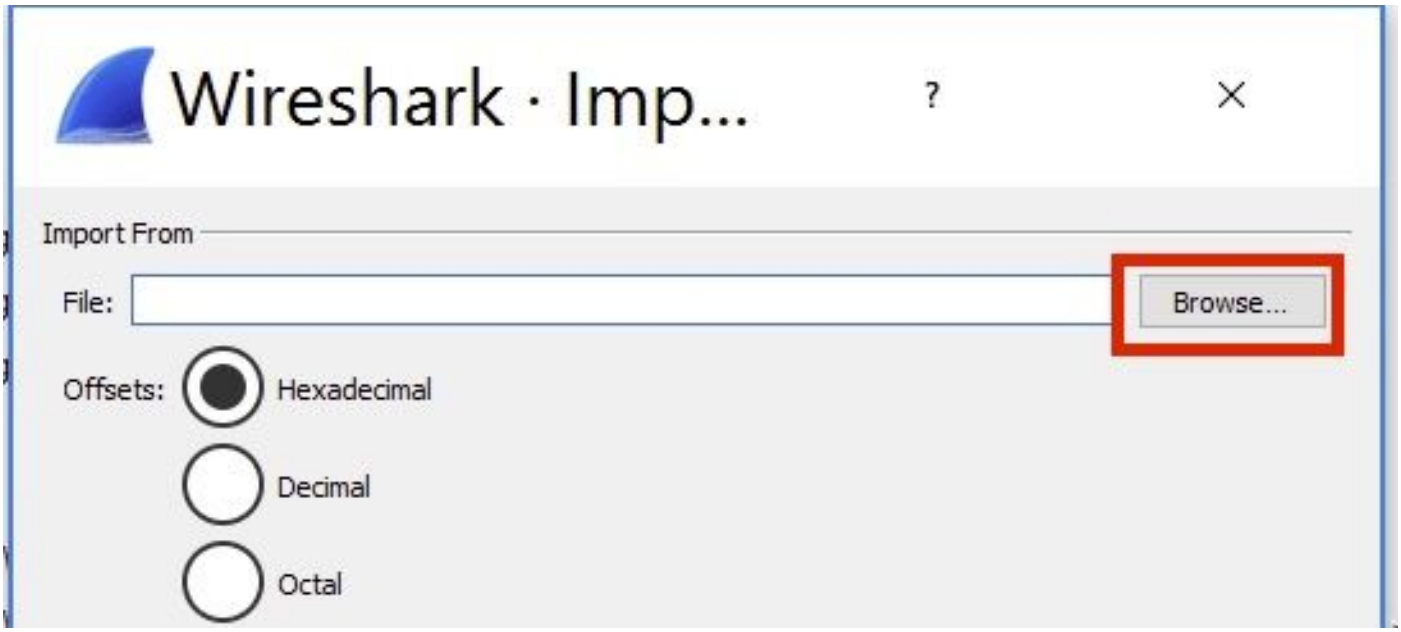
Étape 1. Une fois la sortie terminée, collectez-la et enregistrez-la dans un fichier texte.

Assurez-vous que vous rassemblez un journal propre, sinon Wireshark pourrait afficher des paquets corrompus.

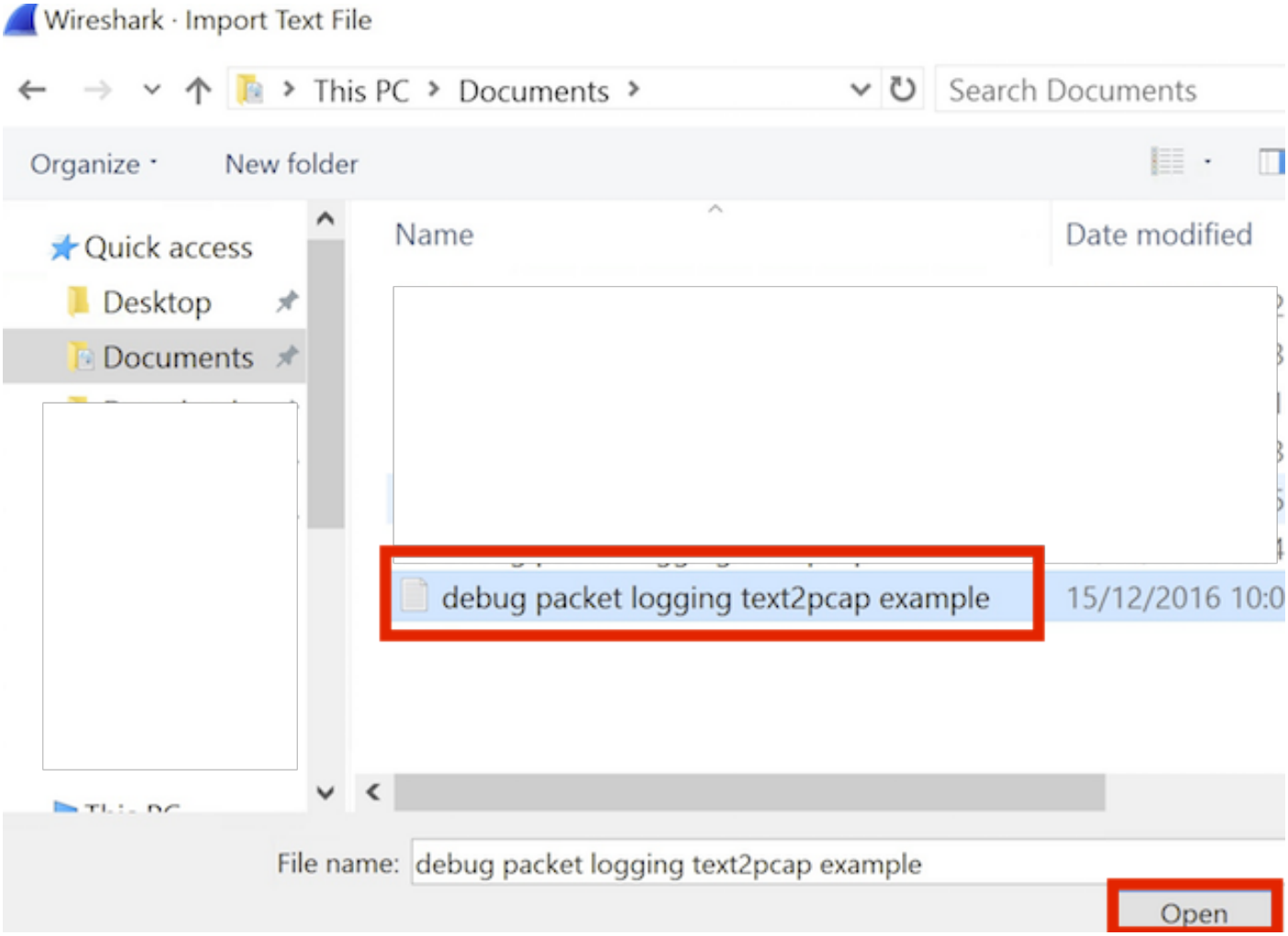
Étape 2. Ouvrez Wireshark et accédez à **Fichier>Importer à partir du vidage hexadécimal...**



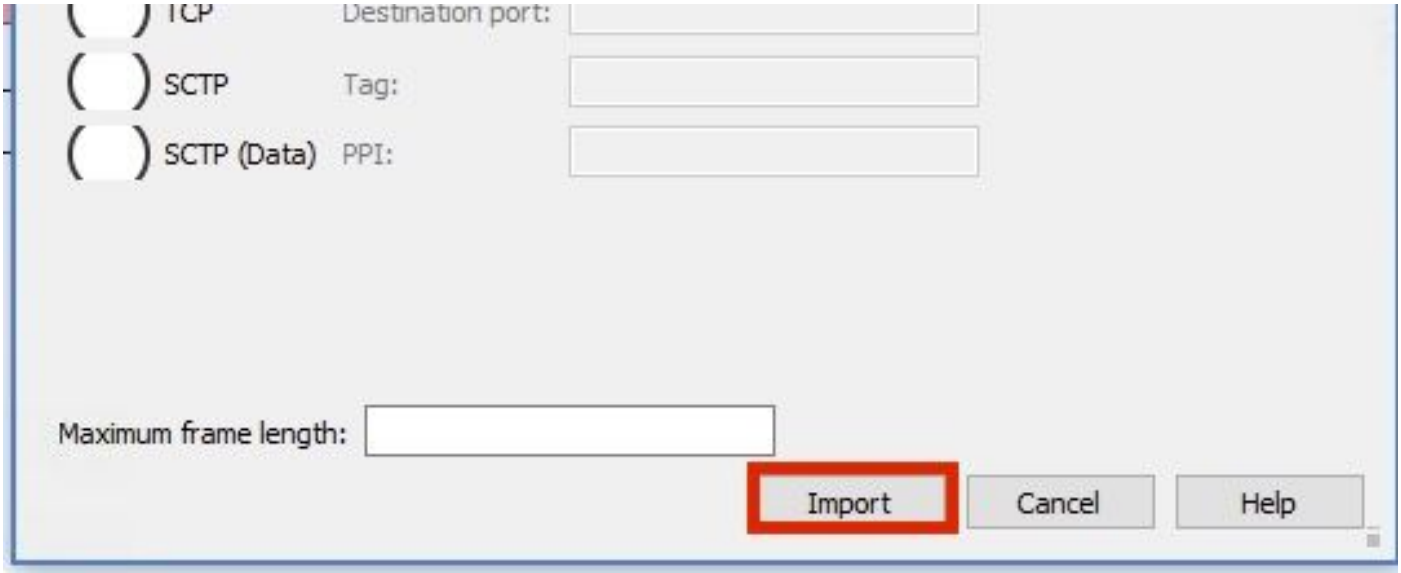
Étape 3. Cliquez sur **Browse.**



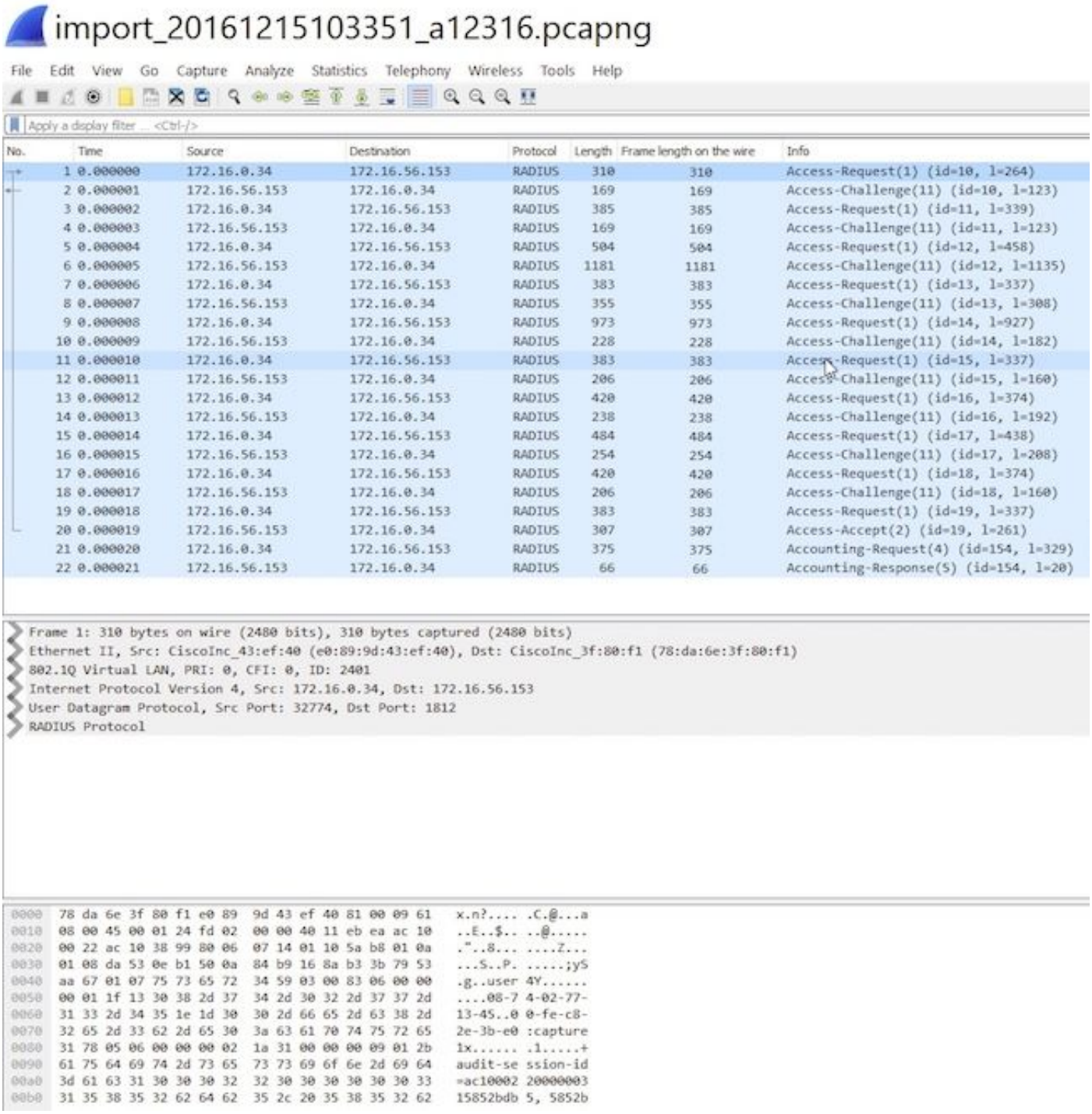
Étape 4. Sélectionnez le fichier texte dans lequel vous avez enregistré la sortie de journalisation des paquets.



Étape 5. Cliquez sur **Import.**



Wireshark affiche le fichier sous la forme .pcap.



Note: Notez que les horodatages ne sont pas exacts et que l'heure delta entre les trames n'est pas exacte.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Vidage de paquets AP
- Notions de base de la norme sans fil 802.11
- Support et documentation techniques - Cisco Systems