

Configuration de la capture de paquets sur le point d'accès WAP121 et WAP321

Objectif

La capture de paquets est une fonctionnalité d'un périphérique réseau qui vous permet de capturer et de stocker des paquets qui sont transmis et reçus par le périphérique. Les paquets capturés peuvent être analysés par un analyseur de protocole réseau pour dépanner ou optimiser les performances. Le fichier de paquets capturé peut être téléchargé via HTTP/HTTPS ou TFTP. Il peut être partagé, puis analysé pour comprendre le flux de paquets dans le réseau.

L'objectif de ce document est d'expliquer comment configurer la capture de paquets et télécharger le fichier de capture de paquets sur les points d'accès WAP121 et WAP321.

Périphériques pertinents

- WAP121
- WAP321

Version du logiciel

- 1.0.3.4 (WAP121 et WAP321)

Configuration de la capture de paquets

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Administration > Packet Capture**. La page *Packet Capture* s'ouvre :

Packet Capture

Packet Capture Configuration

Capture Beacons:	<input checked="" type="checkbox"/> Enable
Promiscuous Capture:	<input type="checkbox"/> Enable
Radio Client Filter:	<input checked="" type="checkbox"/> Enable
Client Filter MAC Address:	4B:DC:88:06:6C:4C (xx:xx:xx:xx:xx:xx)
Packet Capture Method:	<input checked="" type="radio"/> Local File <input type="radio"/> Remote
Capture Interface:	<input type="button" value="▼"/>
Capture Duration:	60 Second (Range: 10-3600, Default: 60)
Maximum Capture File Size:	1024 KB (Range: 64-4096, Default: 1024)
Remote Capture Port:	2002 (Range:1025-65530, Default: 2002)

Étape 2. Cochez la case **Activer** du champ *Capture Beacons*. Les trames de balise sont transmises périodiquement pour annoncer la présence d'un réseau LAN sans fil.

Étape 3. Cochez l'une des cases suivantes en regard de l'un des champs suivants pour choisir une option de capture particulière :

- Promiscuous Capture : la carte d'interface réseau sans fil (NIC) capture tous les paquets, qu'ils soient destinés à ce périphérique ou non.
- Radio Client Filter : fait que la carte réseau sans fil capture les paquets uniquement à partir de clients WLAN.

Remarque : La capture promiscuité et le filtre client radio ne peuvent pas être activés simultanément.

Note: Ignorez l'étape 4 si vous avez choisi le mode de capture promiscuité.

Étape 4. Si le filtre client radio est activé, saisissez l'adresse MAC du filtre client dans le champ *Adresse MAC du filtre client*.

Étape 5. Cliquez sur l'un des boutons d'option *Packet Capture Method*.

- Local File : stocke les paquets capturés sous forme de fichier sur le périphérique AP. Le fichier est au format pcap et le point d'accès peut transférer le fichier vers un serveur TFTP. Ignorez l'étape 7 si vous choisissez cette option.
- Remote : redirige les paquets capturés en temps réel vers un ordinateur externe qui exécute les outils de l'analyseur de protocole réseau. Ignorez l'étape 6 si vous choisissez cette option.

Étape 6. Si Fichier local est sélectionné, configurez ces champs.

Client Filter MAC Address: (xxxxxxxxxxxxxx)

Packet Capture Method: Local File Remote

Capture Interface:

Capture Duration: Second (Range: 10-3600, Default: 60)

Maximum Capture File Size: KB (Range: 64-4096, Default: 1024)

Remote Capture Port: (Range:1025-65530, Default: 2002)

- Capture Interface : sélectionnez l'interface à partir de laquelle les paquets doivent être capturés dans la liste déroulante Capture Interface. La liste déroulante contient les interfaces brtrunk, radio1, eth0 et vap0.
- Capture Duration : saisissez la durée de capture en secondes. Cela peut aller de 10 à 3 600 secondes.
- Taille maximale du fichier de capture : saisissez la taille maximale du fichier de capture (Ko) comprise entre 64 et 4 096 Ko.

Étape 7. Si la méthode Remote Packet Capture est choisie, saisissez le numéro de port compris entre 1 et 65 530 dans le champ Remote Capture Port. Il est défini par défaut à 2002.

Packet Capture

Packet Capture Configuration

Capture Beacons: Enable

Promiscuous Capture: Enable

Radio Client Filter: Enable

Client Filter MAC Address: 00:00:00:00:00:00

Packet Capture Method: Local File
 Remote

Capture Interface: radio1

Capture Duration: 60

Maximum Capture File Size: 1024

Remote Capture Port: 2002

Save

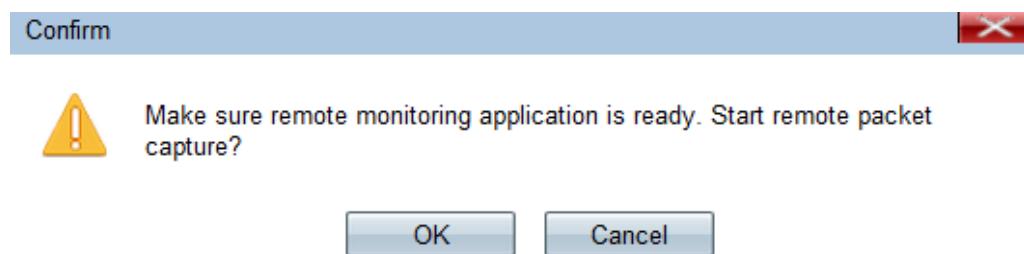
Start Capture

Stop Capture

Étape 8. Cliquez sur **Save** pour enregistrer les paramètres.

Étape 9. Cliquez sur **Start Capture** pour démarrer le processus de capture de paquets.

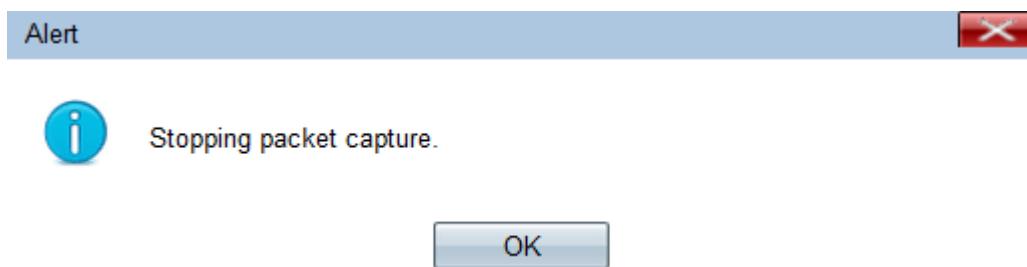
Étape 10. Le message d'alerte s'affiche. Cliquez sur **OK** pour poursuivre le processus de capture de paquets.



Étape 11. Cliquez sur **Stop Capture** pour arrêter le processus de capture de paquets. La zone Packet Capture Status indique que la capture est en cours.

Save	Start Capture	Stop Capture
Packet Capture Status		
Current Capture Status:	File capture in progress	
Packet Capture Time:	0	
Packet Capture File Size:	0 KB	
<input type="button" value="Refresh"/>		

Étape 12. Le message d'alerte s'affiche. Cliquez sur **OK** pour arrêter le processus de capture de paquets.



État de la capture de paquets

Étape 1. La zone Packet Capture Status contient les informations suivantes. Cliquez sur **Actualiser** pour obtenir le statut récent.

Save	Start Capture	Stop Capture
Packet Capture Status		
Current Capture Status:	File capture in progress	
Packet Capture Time:	0	
Packet Capture File Size:	0 KB	
<input type="button" value="Refresh"/>		

· Current Capture Status : affiche l'état actuel de la capture de paquets.

· Packet Capture Time : affiche l'heure à laquelle les paquets sont capturés.

· Packet Capture File Size : affiche la taille du fichier de capture de paquet.

Téléchargement du fichier de capture de paquets

Étape 1. (Facultatif) Si le fichier capturé doit être téléchargé via un serveur TFTP, cochez la case **Utiliser TFTP pour télécharger le fichier de capture**. Le champ Nom de fichier du

serveur TFTP et les champs Adresse IPv4 du serveur TFTP s'activent.

Packet Capture File Download

File download using HTTP/HTTPS may be done by simply clicking the Download button. To use TFTP download, Use TFTP to download the capture file

TFTP Server Filename: (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

Économiseur de temps : Si vous ne cochez pas la case de l'étape 1, passez à l'étape 4.

Étape 2. Entrez le nom de fichier au format pcap dans le champ Nom de fichier du serveur TFTP.

Étape 3. Entrez l'adresse IPv4 du serveur TFTP dans le champ TFTP Server IPv4 Address.

Étape 4. Cliquez sur Download. Si vous n'avez pas choisi TFTP, le fichier est téléchargé avec HTTP/HTTPS, une fenêtre s'affiche pour vous informer que le téléchargement est en cours. Click OK.

Capture Duration: Second (Range: 10-3600, Default: 60)

Maximum Capture File Size:

Remote Capture Port:

Packet Capture Status

Current Capture Status: Stopped due to administrative action

Packet Capture Time: 00:00:13

Packet Capture File Size: 213 KB

Packet Capture File Download

File download using HTTP/HTTPS may be done by simply clicking the Download button. To use TFTP download, check the box Use TFTP to download the capture file

TFTP Server Filename: (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

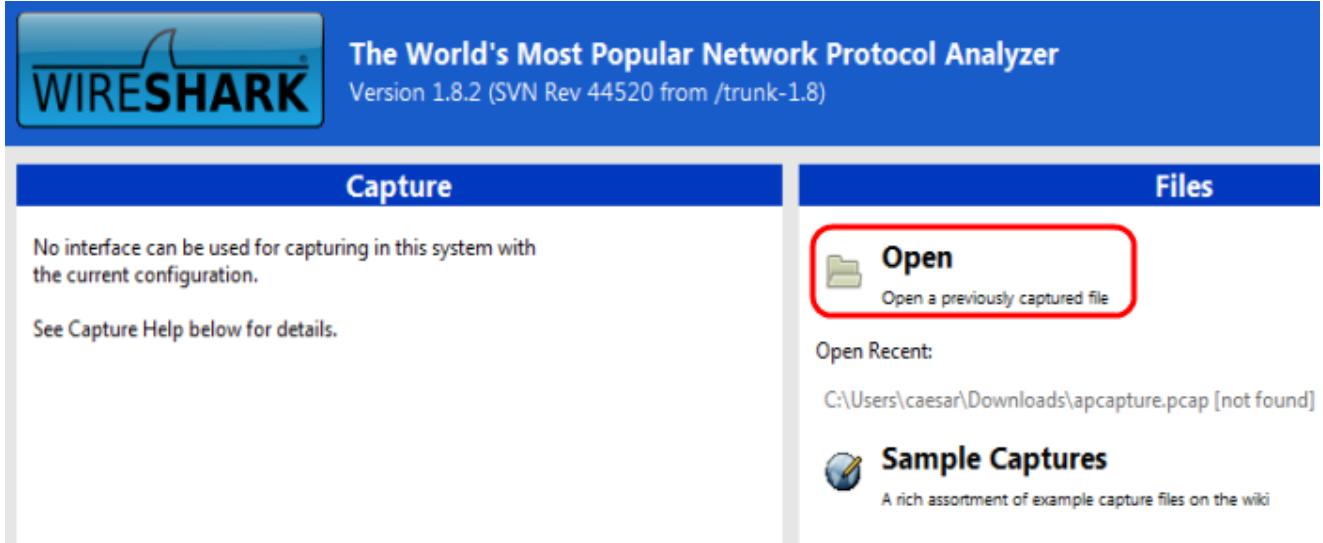
Confirm

 The file is downloading now.

Remarque : vous pouvez utiliser le logiciel Wireshark, qui est open source, pour interpréter et comprendre les informations obtenues à partir de la capture de paquets.

Afficher le paquet capturé dans Wireshark

Étape 1. Lancez le logiciel Wireshark.



Étape 2. Cliquez sur **Ouvrir** dans la section Fichier pour parcourir et sélectionner le fichier de capture à partir de votre ordinateur.

Étape 3. Recherchez le fichier sur le PC.

Étape 4. Ouvrir pour afficher le fichier capturé.