Configurer la capture de paquets pour optimiser les performances sur un point d'accès sans fil

Objectif

La fonction de capture de paquets permet de capturer et de stocker les paquets reçus et transmis par le point d'accès sans fil (WAP). Cette fonctionnalité est très utile pour le dépannage ou l'optimisation des performances, car les paquets capturés peuvent ensuite être analysés par un analyseur de protocole réseau. Il existe deux méthodes de capture de paquets :

- Méthode de capture locale : les paquets capturés sont stockés dans un fichier sur le WAP. Le WAP peut également envoyer le fichier à un serveur TFTP (Trivial File Transport Protocol). Le fichier Administration Packet Capture est formaté au format pcap et peut être examiné à l'aide d'outils logiciels d'analyse de paquets tels que Wireshark et OmniPeek.
- Méthode de capture à distance : les paquets capturés sont redirigés en temps réel vers un ordinateur externe exécutant l'outil Wireshark.

Cet article vise à vous guider dans la configuration de la capture de paquets sur un WAP et à recevoir ces captures de paquets localement ou à distance. Une fois cette opération effectuée, vous pouvez vérifier l'état de la capture de paquets, puis télécharger le fichier.

Périphériques pertinents

- Points d'accès sans fil

Version du logiciel

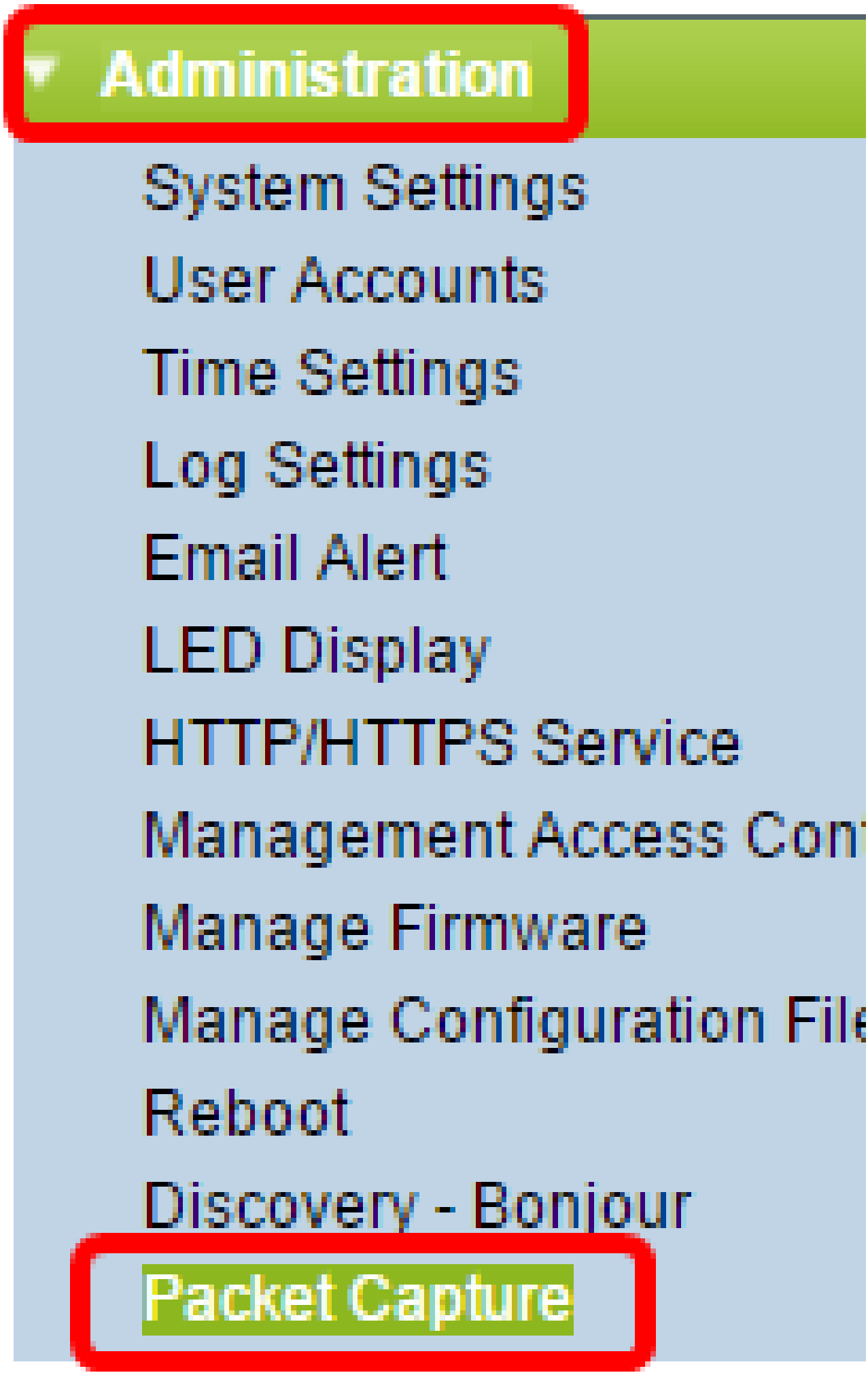
- 1.0.1.2 : WAP150, WAP361
- 1.0.2.2 : WAP351, WAP131
- 1.0.6.2 : WAP121, WAP321
- 1.2.1.3 : WAP371, WAP551, WAP561
- 1.0.0.17 - WAP571, WAP571E

Configurer la capture de paquets

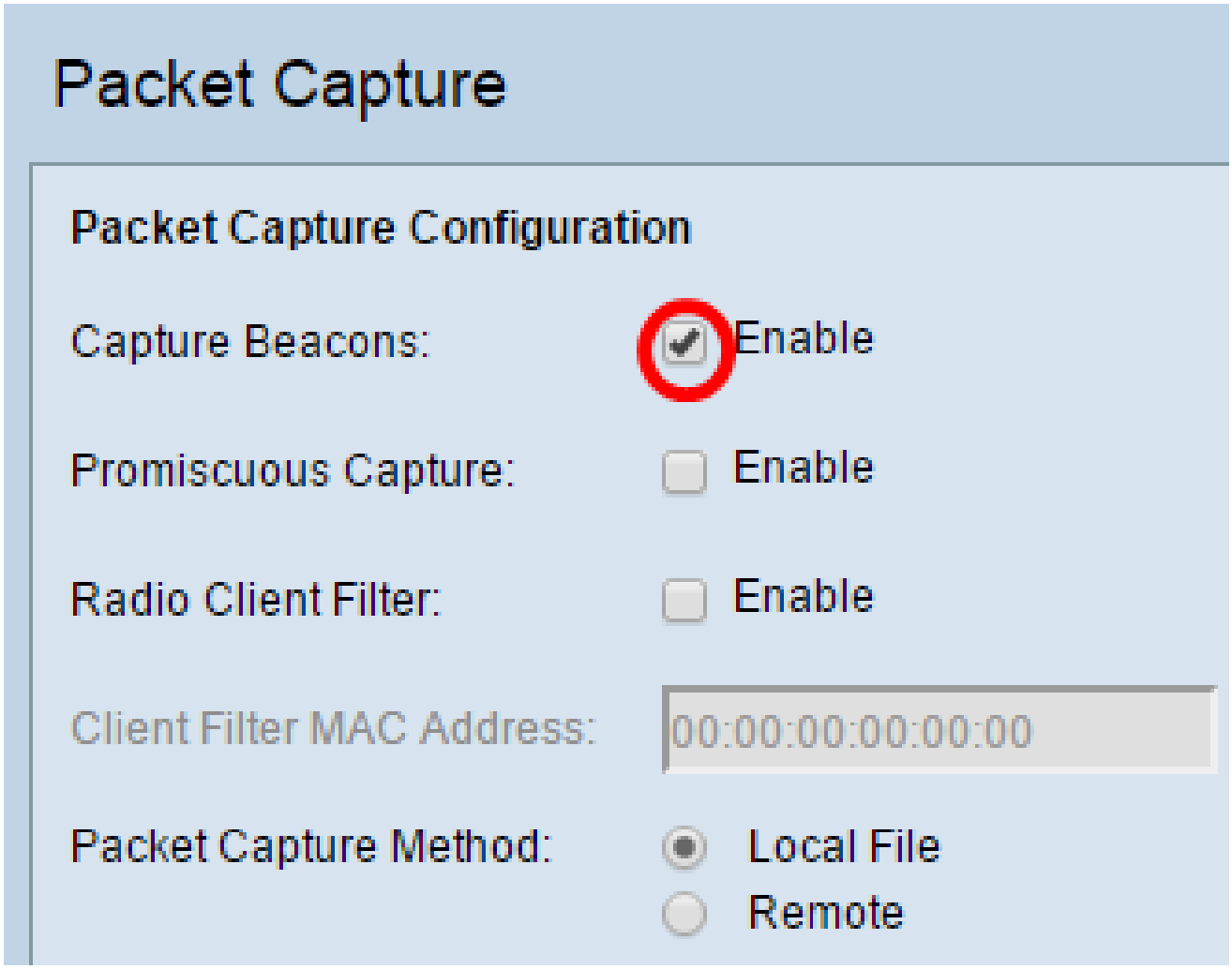
Configuration des paramètres de capture de paquets

Étape 1. Connectez-vous à l'utilitaire Web de votre point d'accès et choisissez Administration > Packet Capture.

Remarque : les onglets peuvent varier en fonction du modèle WAP que vous utilisez. Les images ci-dessous proviennent de WAP361.

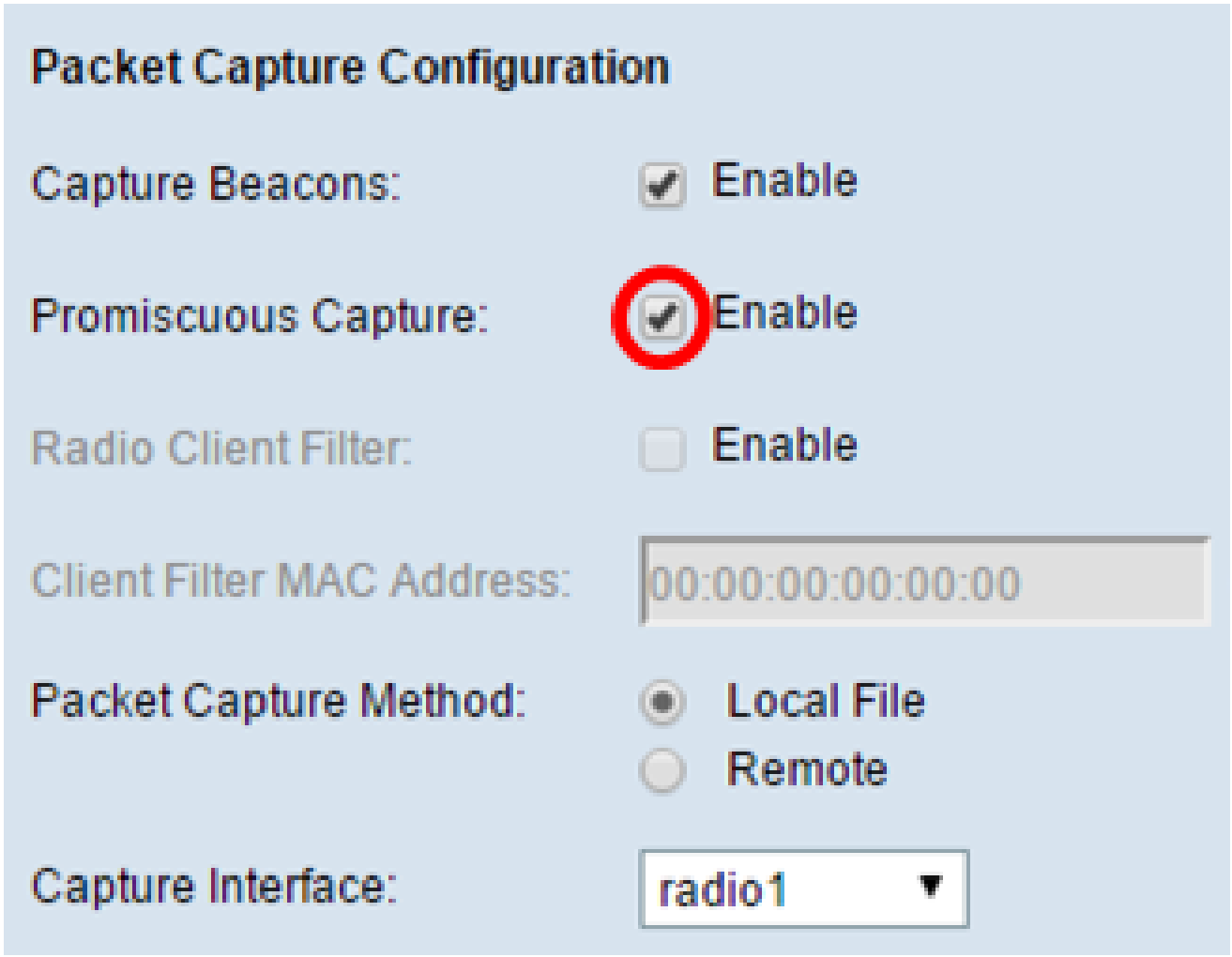

Administration
System Settings
User Accounts
Time Settings
Log Settings
Email Alert
LED Display
HTTP/HTTPS Service
Management Access Con
Manage Firmware
Manage Configuration File
Reboot
Discovery - Bonjour
Packet Capture

Étape 2. Vérifiez si la case Enable dans Capture Beacons est cochée. Les trames de balise sont transmises périodiquement pour annoncer la présence d'un réseau local sans fil (WLAN). Cette fonction est activée par défaut.



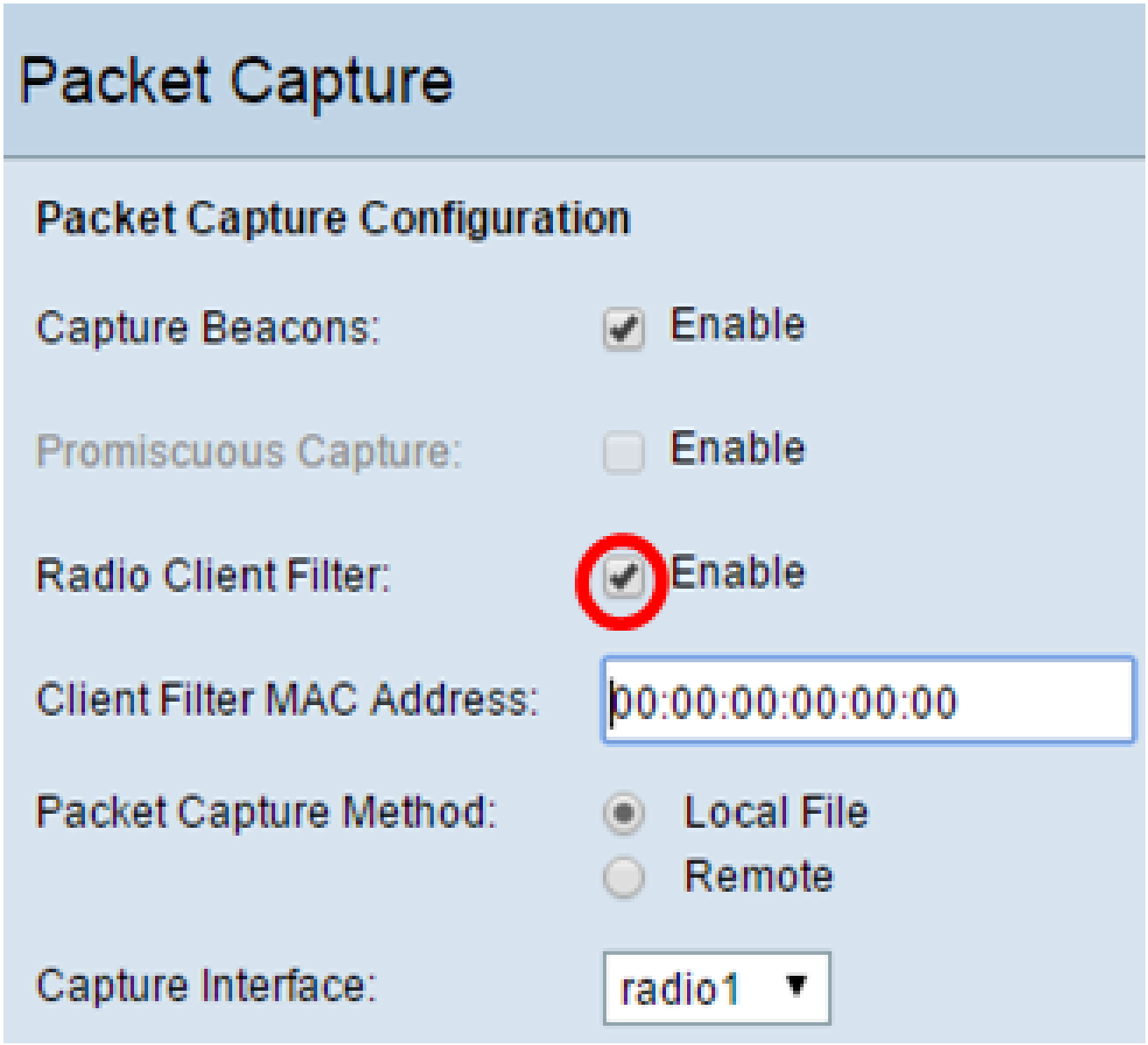
Remarque : les protocoles WAP551 et WAP561 capturent trois types de paquets : les paquets associés au réseau local sans fil, le réseau local Ethernet et les paquets aux interfaces internes.

Étape 3. (Facultatif) Si vous souhaitez activer une carte réseau sans fil pour capturer les paquets associés à un WAP, cochez la case Enable de Promiscuous Capture. Si vous cochez cette case, passez à l'étape 6.

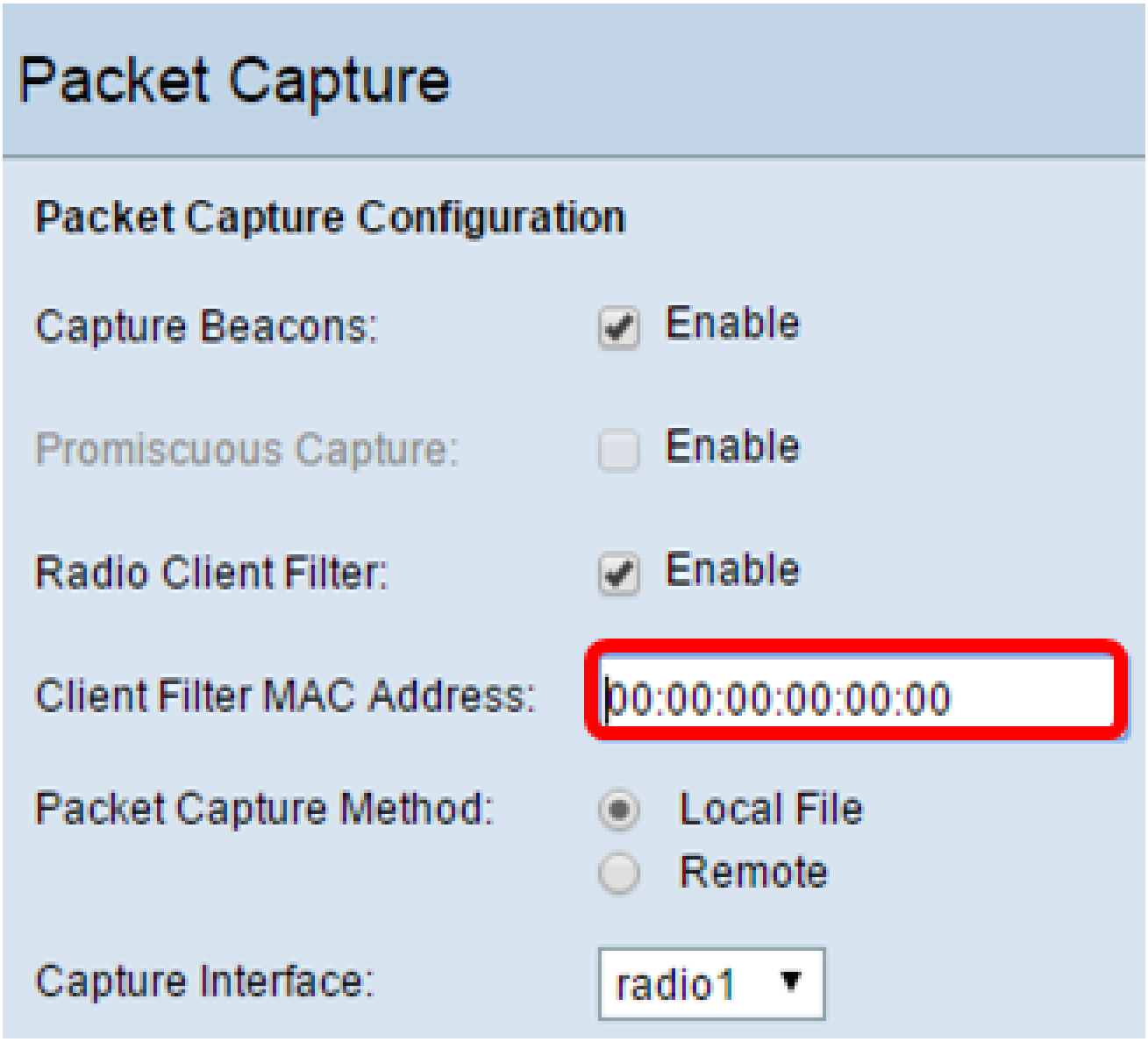


Remarque : la fonction Capture promiscuité ou Filtre client radio peut être activée.

Étape 4. (Facultatif) Si vous n'avez pas coché la case Capture promiscuité et que vous souhaitez activer une carte réseau sans fil pour capturer des paquets sans devoir les associer à un WAP, cochez la case Enable du Radio Client Filter.

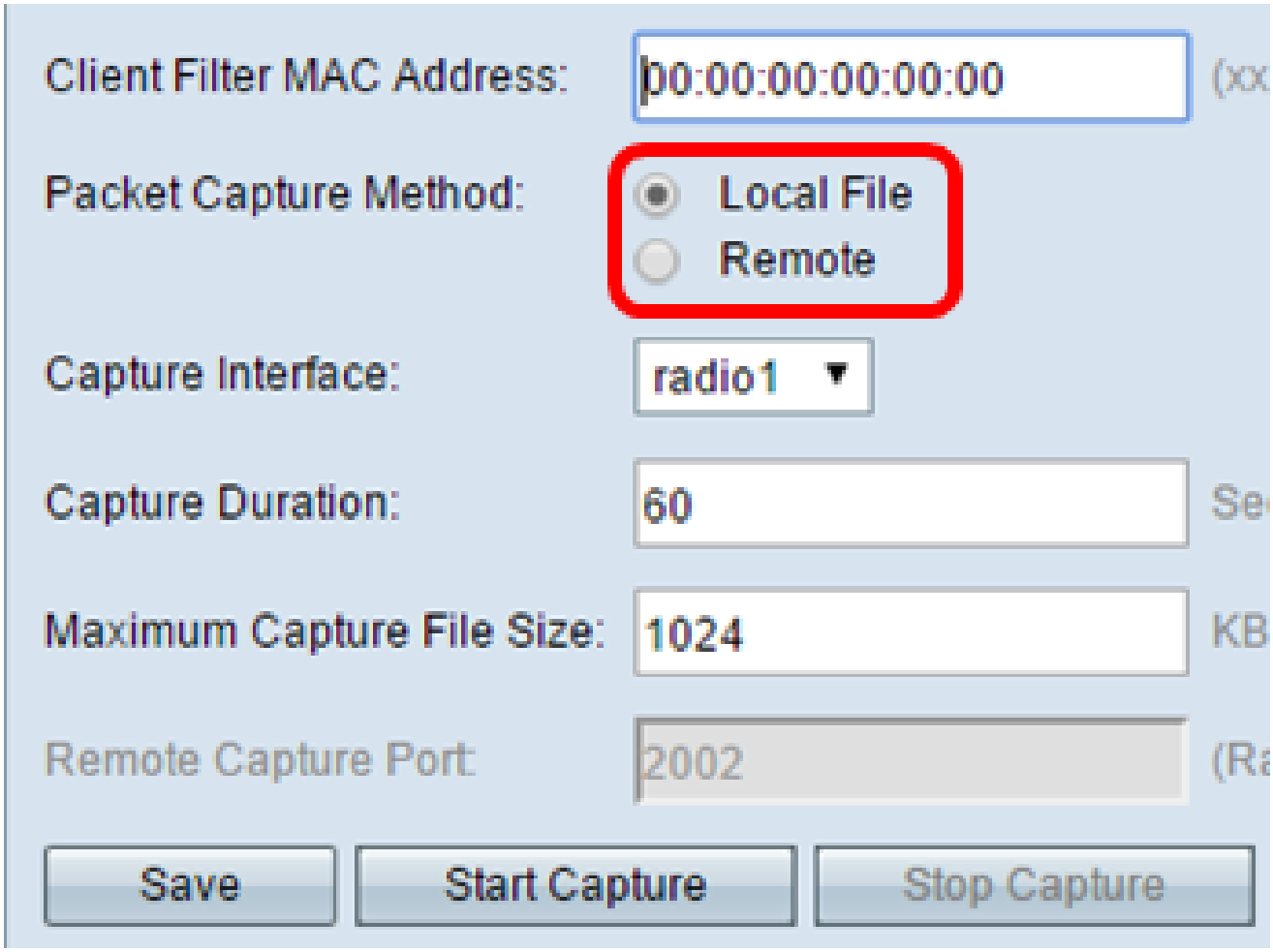


Étape 5. (Facultatif) Si Radio Client Filter est activé, saisissez l’adresse MAC du filtre client dans le champ Client Filter MAC Address.

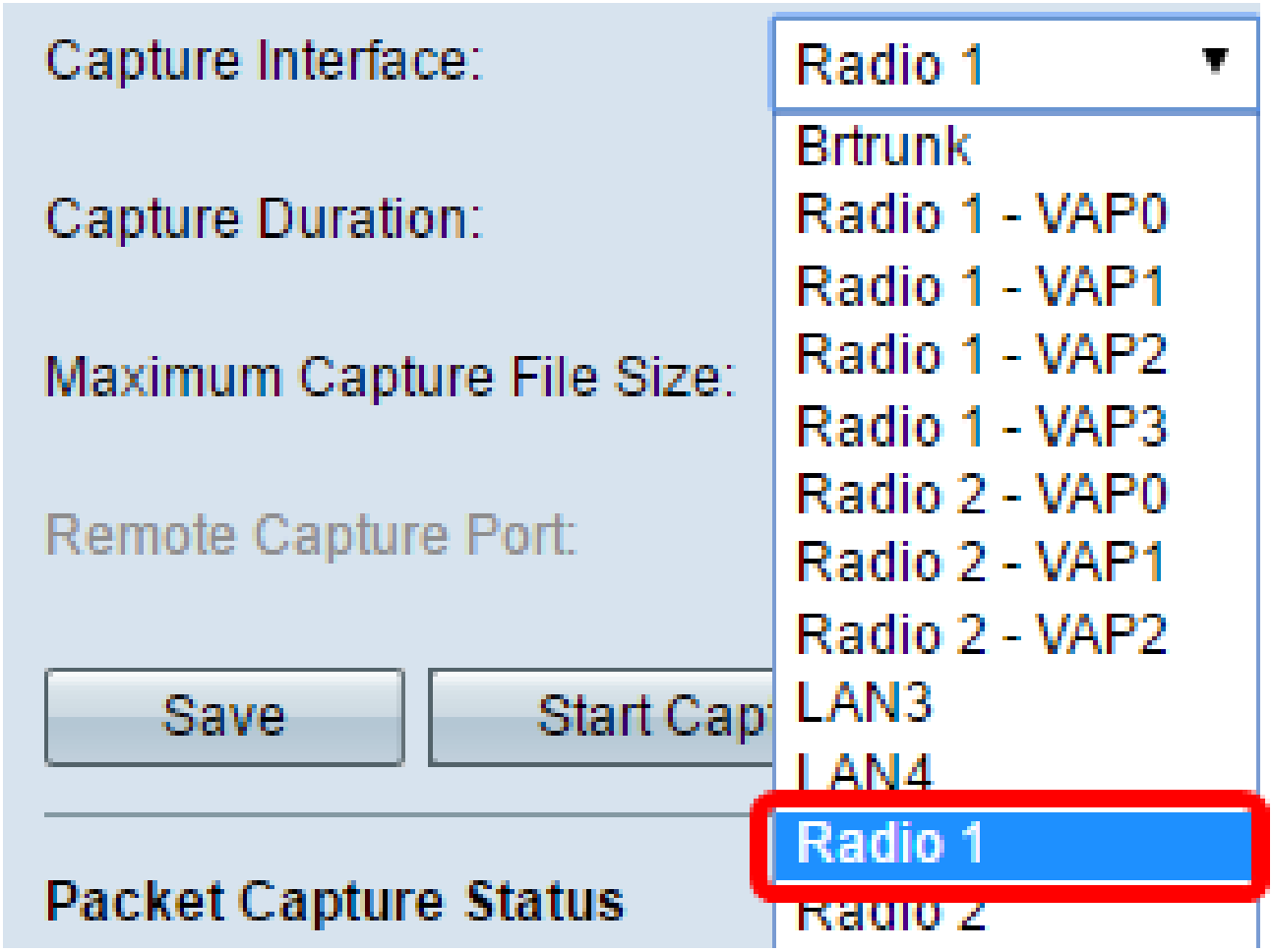


Étape 6. Sélectionnez l'une des cases d'option Packet Capture Method suivantes :

- Local File : stocke les paquets capturés sous la forme d'un fichier sur le WAP. Si cette option est sélectionnée, passez à l'étape suivante.
- Remote : redirige les paquets capturés en temps réel vers un ordinateur externe qui exécute les outils d'analyse de protocole réseau. Si cette option est sélectionnée, passez à l'étape 10.



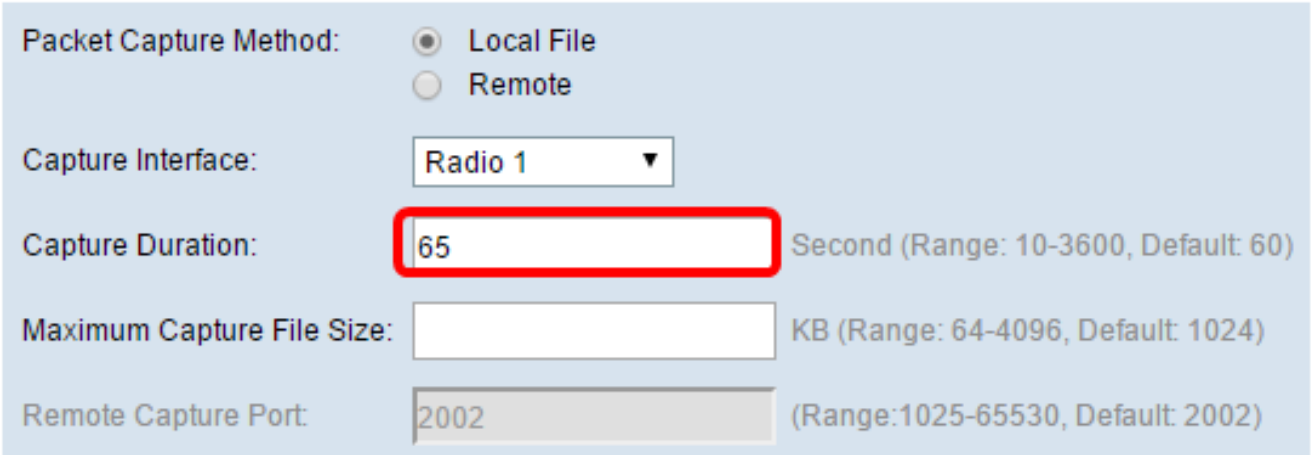
Étape 7. (Facultatif) Si vous choisissez la méthode de capture Fichier local, choisissez l'interface pour laquelle les paquets doivent être capturés dans la liste déroulante Interface de capture. La liste des options peut varier en fonction du modèle WAP que vous utilisez.



- Radio 1/Radio 2 : trafic 802.11 sur l'interface radio
- Ethernet/eth0 : trafic 802.3 sur le port Ethernet
- Radio 1 - VAP0/Radio 2 - VAP0 - Trafic VAP0
- Radio 1 - VAP1 à Radio 1 - VAP3 (si configuré) - Trafic sur le point d'accès virtuel (VAP) spécifié
- Radio 2 - VAP1 à Radio 2 - VAP3 (si configuré) - Trafic sur le VAP spécifié
- Radio 1 - WDS0 vers Radio 1 - WDS3 (si configuré) - Trafic sur le système de distribution sans fil (WDS) spécifié
- Radio 2 - WDS0 vers Radio 2 - WDS3 (si configuré) - Trafic sur le WDS spécifié
- LAN1 à LAN5 : trafic 802.3 sur le port Ethernet
- Brtrunk : interface de pont Linux dans le périphérique WAP.
- wlan0vap1 à wlan0vap7 — Trafic sur le VAP spécifié sur Radio 1
- wlan1vap1 à wlan1vap7 — Trafic sur le VAP spécifié sur Radio 2
- wlan0wds0 à wlan0wds3 — Trafic sur l'interface WDS spécifiée
- VAP0 ou WLAN0:VAP0 — Trafic VAP0
- WLAN1:VAP0 — Trafic VAP0 sur Radio 2 (pour les périphériques WAP561 uniquement)
- wlan1 — Trafic VAP0 sur Radio 2
- Radio 1 - VAP1 à Radio 1 - VAP7 (si configuré) - Trafic sur le VAP spécifié
- Radio 2 - VAP1 à Radio 2 - VAP7 (si configuré) - Trafic sur le VAP spécifié

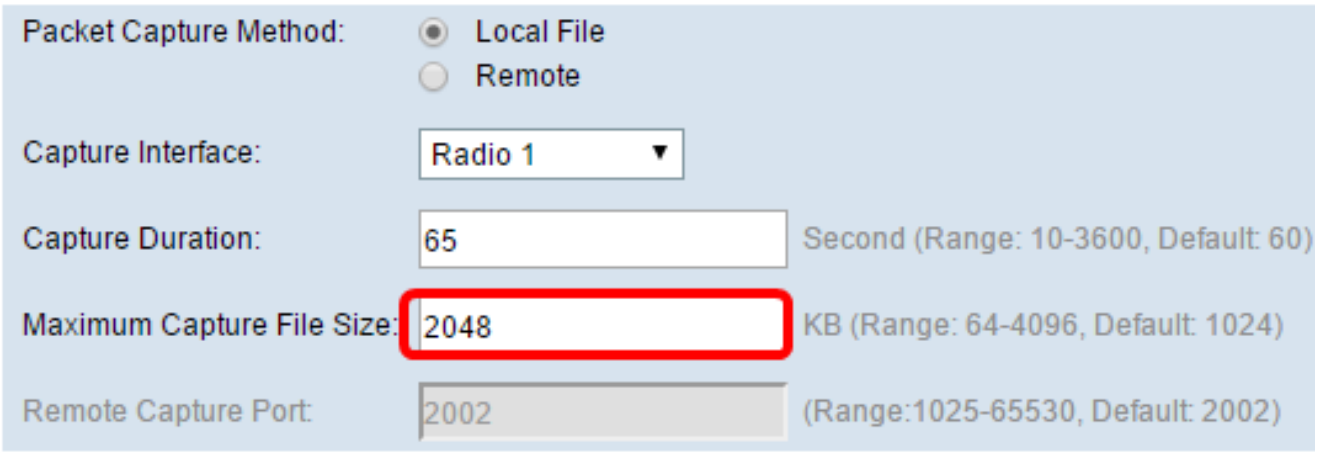
Étape 8. Saisissez une durée de capture comprise entre 10 et 3 600 secondes dans le champ Capture Duration. La valeur par défaut est de 60 secondes.

Remarque : Dans cet exemple, l'adresse IP 65 est utilisée.

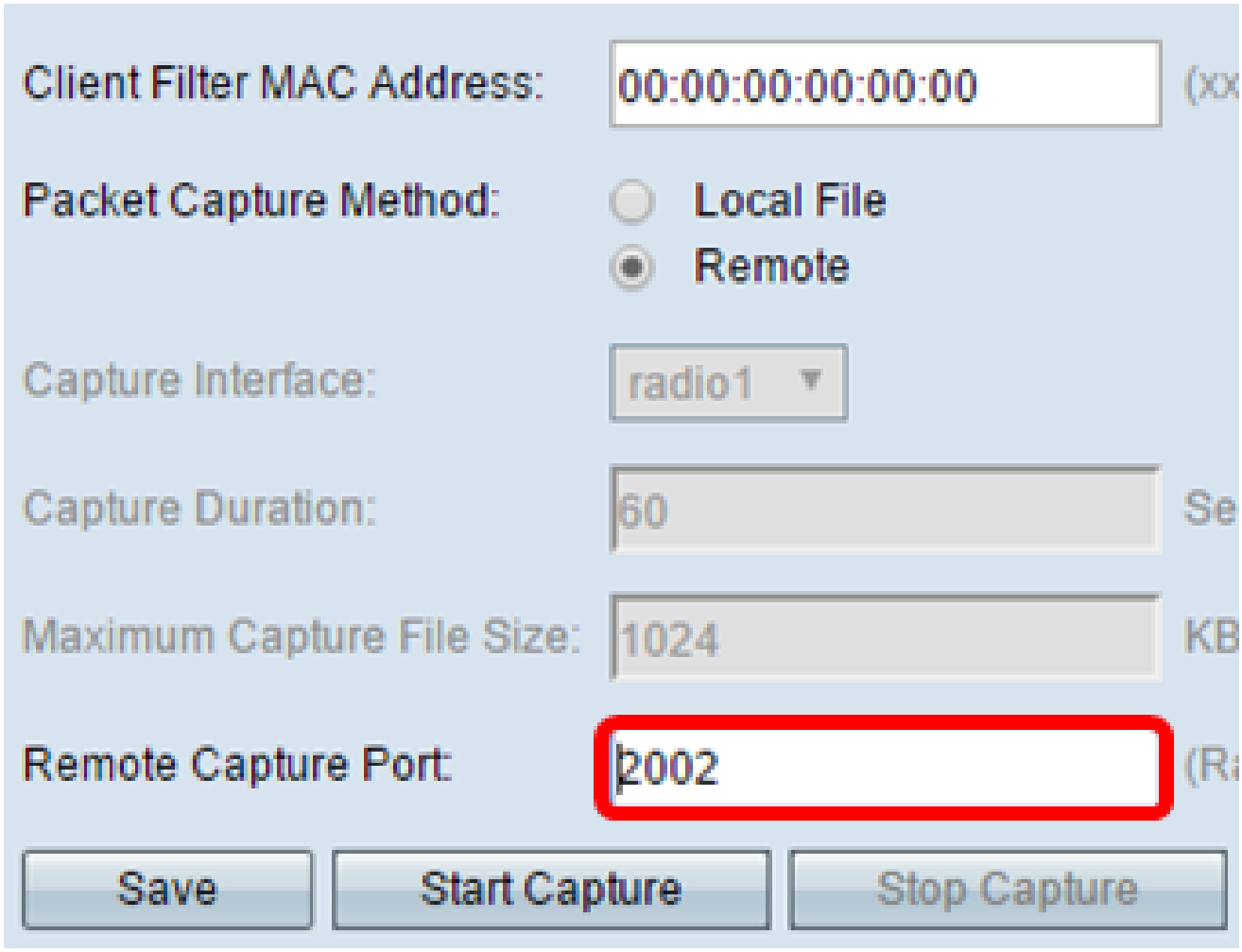


Étape 9. Saisissez la taille maximale du fichier de capture, comprise entre 64 et 4 096 Ko, dans le champ Taille maximale du fichier de capture. La valeur par défaut est 1 024 Ko.

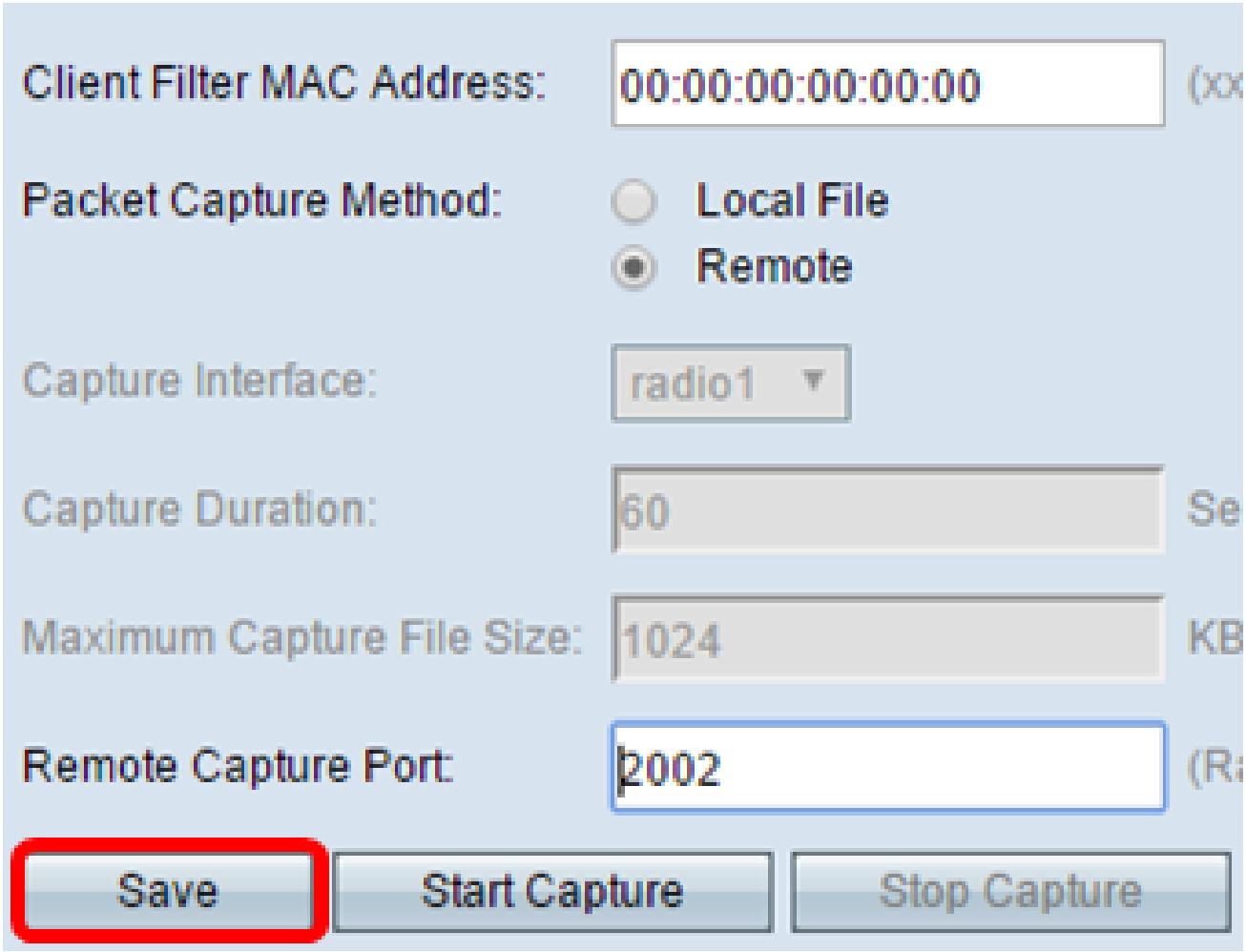
Remarque : Dans cet exemple, l'adresse IP 2048 est utilisée.



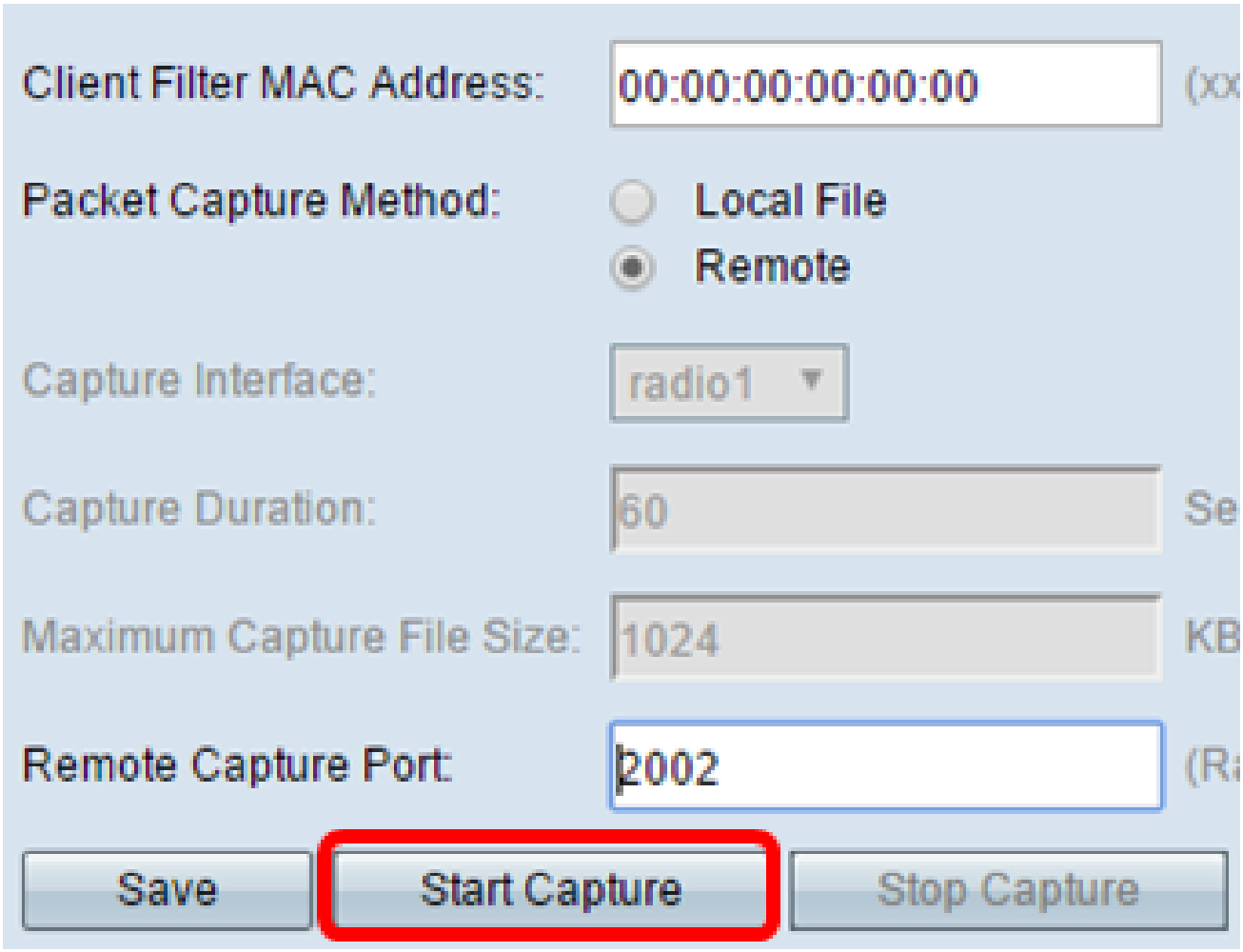
Étape 10. (Facultatif) Si vous choisissez la méthode de capture de paquets distants, saisissez le numéro de port compris entre 1 et 65530 dans le champ Remote Capture Port. La valeur par défaut est 2002.



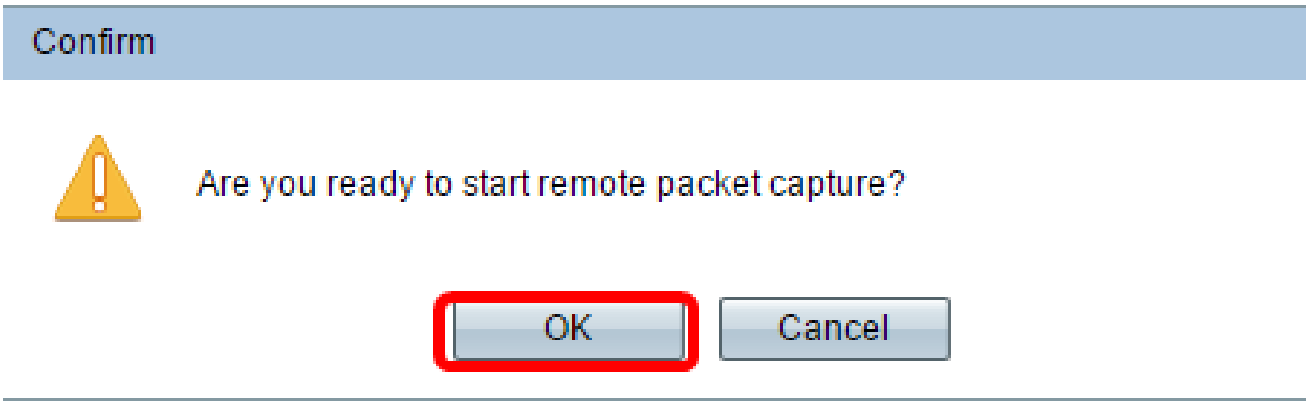
Étape 11. Cliquez sur Save.



Étape 12. Cliquez sur Start Capture pour lancer le processus de capture de paquets.



Étape 13. Une fois que la fenêtre de confirmation s'affiche, cliquez sur OK.



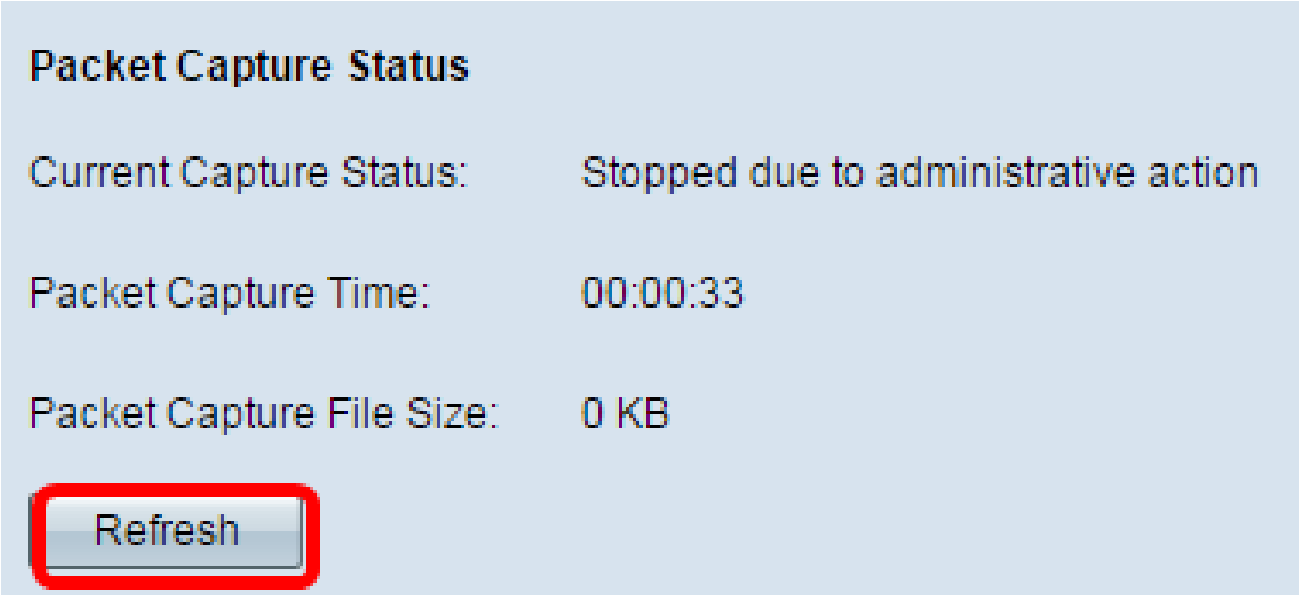
Remarque : la zone Packet Capture Status indique que la capture est en cours.

Étape 14. (Facultatif) Cliquez sur Stop Capture pour arrêter le processus de capture de paquets, puis cliquez sur OK.

Vous venez de configurer les paramètres de capture de paquets.

État de capture des paquets

La zone Packet Capture Status contient les informations suivantes. Cliquez sur Refresh pour afficher l'état récent.



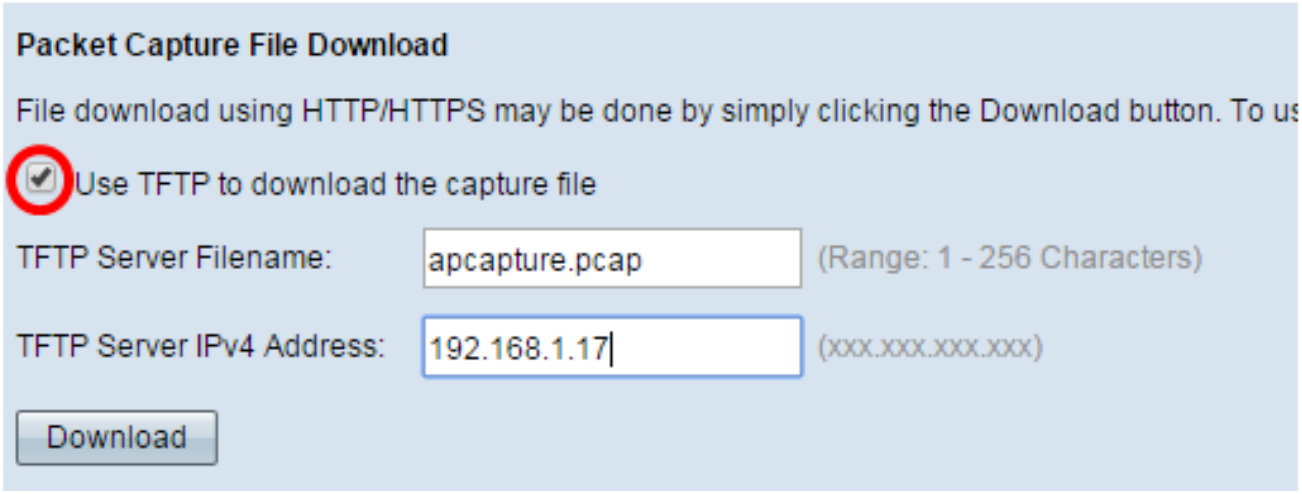
- Current Capture Status : affiche l'état actuel de capture des paquets.
- Packet Capture Time : affiche la durée pendant laquelle les paquets sont capturés.
- Packet Capture File Size : affiche la taille du fichier de capture de paquets.

Téléchargement du fichier de capture de paquets

Il existe deux façons de télécharger le fichier de capture de paquets.

- Hypertext Transfer Protocol (HTTP)
- Trivial File Transfer Protocol (TFTP)

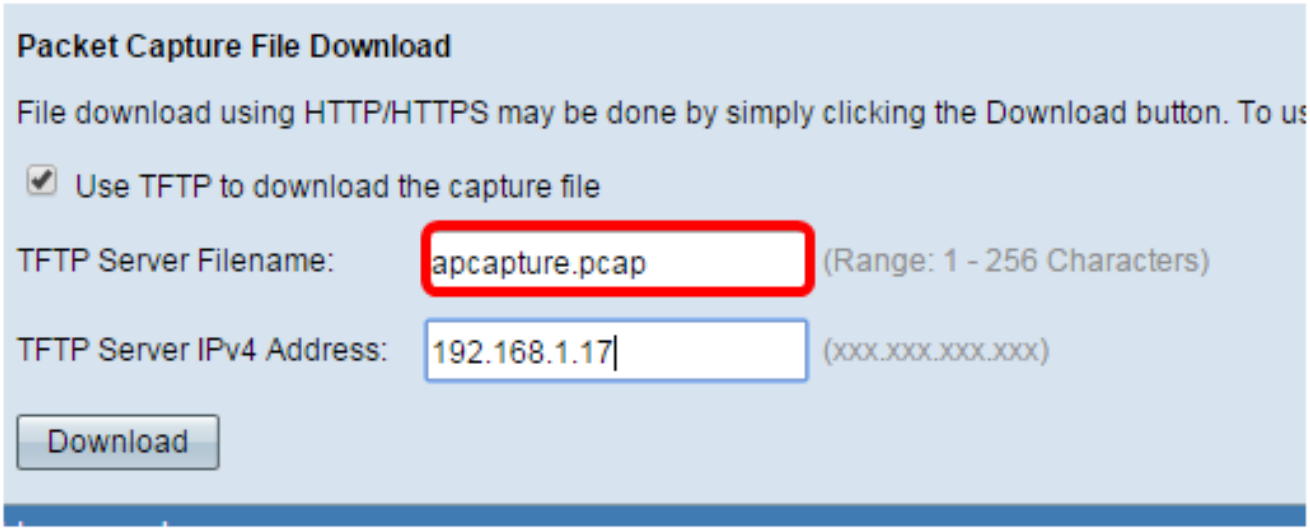
Étape 1. (Facultatif) Si le fichier capturé doit être téléchargé via un serveur TFTP, cochez la case Utiliser TFTP pour télécharger le fichier de capture. Lorsque cette case est cochée, les champs TFTP Server Filename et TFTP Server IPv4 Address s'activent.



Remarque : si vous n'avez pas coché la case à cocher de l'étape 1, passez à l'étape 4.

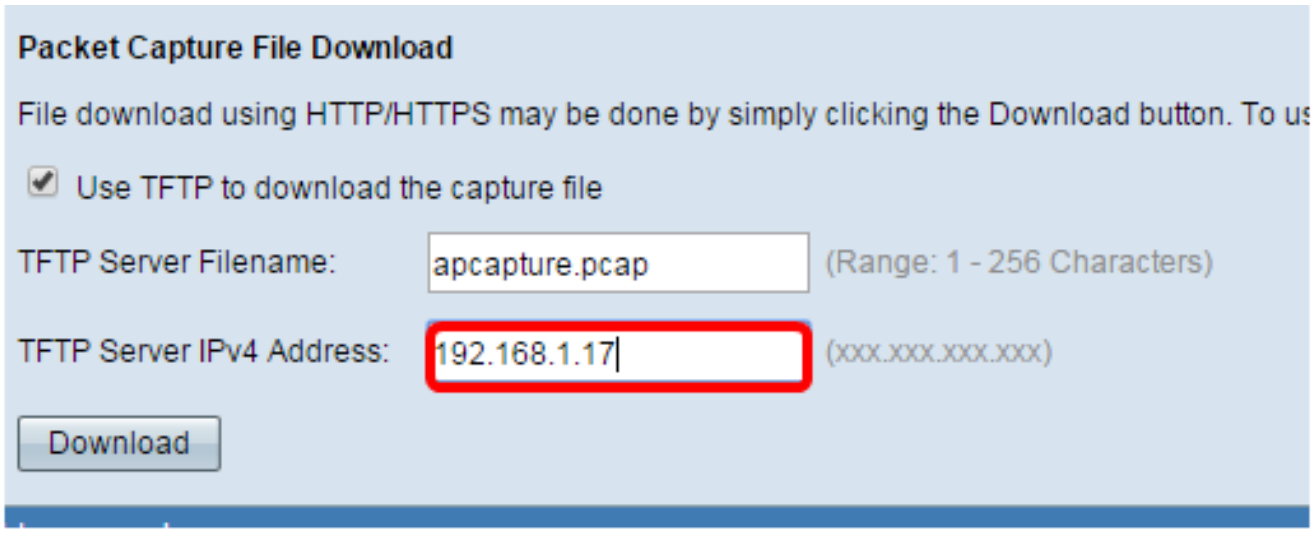
Étape 2. Entrez le nom de fichier au format pcap dans le champ TFTP Server Filename qui comporte entre 1 et 256 caractères.

Remarque : dans cet exemple, apcapture.pcap est utilisé.



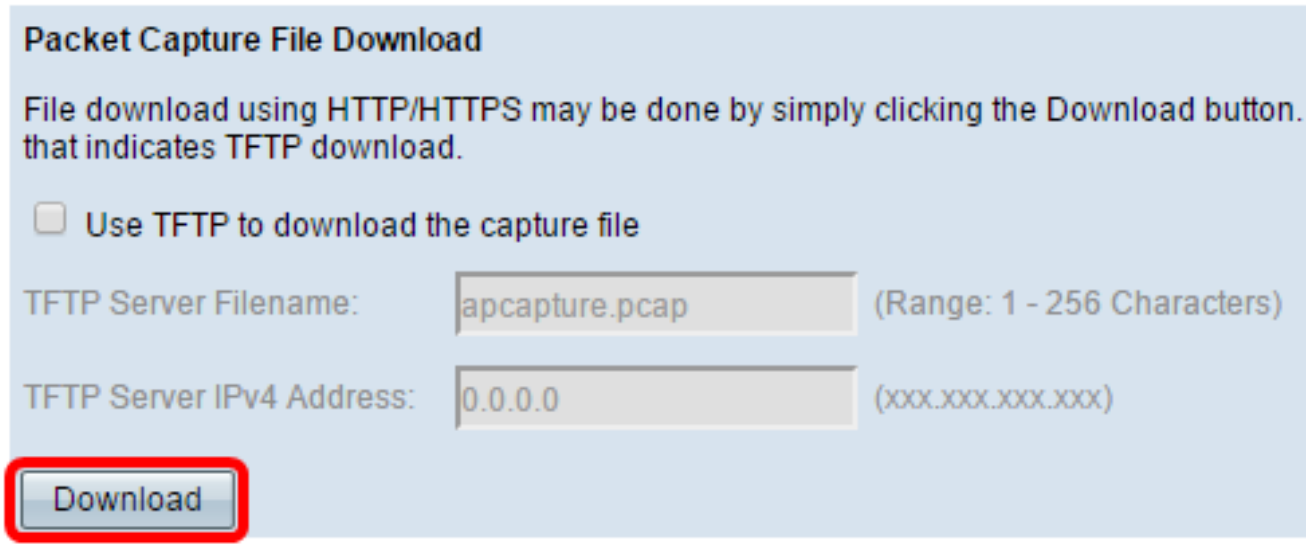
Étape 3. Saisissez l'adresse IPv4 du serveur TFTP dans le champ TFTP Server IPv4 Address.

Remarque : dans cet exemple, 192.168.1.17 est utilisé.

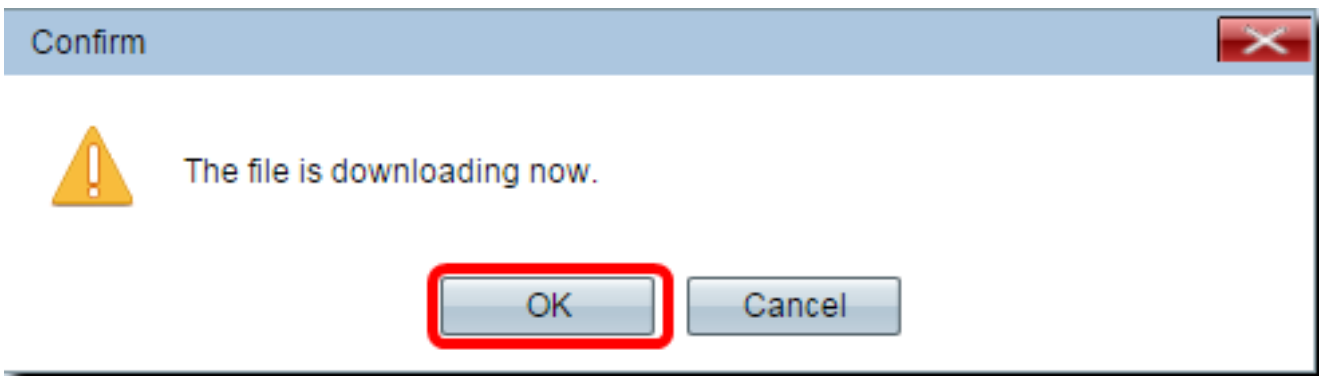


Étape 4. Cliquez sur Download.

Remarque : si vous n'avez pas choisi TFTP, le fichier est téléchargé via HTTP/HTTPS.



Étape 5. Une fenêtre s'affiche pour vous informer que le téléchargement est en cours. Click OK.



Vous devez maintenant avoir téléchargé votre fichier de capture de paquets via HTTP/HTTPS ou TFTP.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.