

Capture de paquets intégrée dans les commutateurs Catalyst 1200 et 1300

Objectif

L'objectif de cet article est de passer en revue la nouvelle fonctionnalité de capture de paquets embarquée (OPC) dans les commutateurs Catalyst 1200 et 1300 sur la version 4.1.3.36 du microprogramme. Dans ce micrologiciel, l'OPC ne peut être configuré qu'à l'aide de l'interface de ligne de commande (CLI).

Périphériques pertinents | Version du logiciel

- Commutateurs Catalyst 1200 | 4.1.3.36
- Commutateurs Catalyst 1300 | 4.1.3.36

Introduction

Dans la version 4.1.3.36 du microprogramme des commutateurs Catalyst 1200 et 1300, une nouvelle fonctionnalité appelée OPC (Onboard Packet Feature) a été introduite. Lorsque cette option est activée, OPC alloue jusqu'à 20 Mo de mémoire pour la capture des paquets de données. Cette fonctionnalité nécessite la configuration d'un point de capture qui définit le comportement d'une instance OPC. Le point de capture permet de définir tous les paramètres associés à une instance OPC. La fonctionnalité OPC améliore les fonctionnalités de dépannage sur le périphérique.

Dans ce micrologiciel, OPC ne peut être configuré qu'à l'aide de l'interface de ligne de commande. Les points de capture sont configurés en mode d'exécution privilégié et ne peuvent pas être enregistrés dans les fichiers de configuration du commutateur, pas plus que les paramètres après un redémarrage du commutateur.

Un maximum de 4 points de capture peut être configuré sur un commutateur, mais un seul point de capture peut être actif à la fois. La capture de paquets est prise en charge pour l'interface du plan de contrôle (CPU). Les données capturées en mémoire peuvent être enregistrées dans la mémoire flash intégrée si l'espace est libre, ou sur un périphérique USB connecté tel qu'un lecteur flash USB. Comme OPC peut consommer des ressources CPU considérables, il est recommandé de l'utiliser uniquement en cas de besoin.

Table des matières

- [Commandes de configuration des points de capture](#)
- [Paramètres du tampon](#)
- [Paramètres d'interface source](#)
- [Capturer les paramètres de filtre](#)
- [Démarrage et arrêt de la capture](#)
- [Enregistrement des données de capture de paquets](#)

Commandes de configuration des points de capture

Étape 1

Un point de capture peut être créé à l'aide de la commande `monitor capture {capture-name}`.

```
monitor capture cap1
```

Dans l'exemple ci-dessus, un point de capture nommé `cap1` a été créé.

Étape 2

Pour afficher les détails d'un point de capture configuré, tapez la commande `show monitor capture {capture-name}`.

```
show monitor capture cap1
```

Note:

Vous pouvez afficher tous les points de capture actuellement configurés à l'aide de la commande `show monitor capture` sans spécifier de nom de capture.

```
switch4ac12e#monitor capture cap1
switch4ac12e#show monitor capture

Status Information for Capture cap1
  Target Type:
  Interface: None, Direction: NONE
  Status : Inactive
  Filter Details:
    None
  Buffer Details:
    Buffer Type: LINEAR (default)
    Buffer size (in MB): 5 (default)
```

Étape 3

Pour supprimer un point de capture, utilisez la commande `no monitor capture {capture-name}`.

```
no monitor capture cap1
```

```
Buffer size (in MB): 5 (default)
switch4ac12e#no monitor capture cap1
switch4ac12e#show monitor capture
No capture exist
switch4ac12e#
```

Paramètres du tampon

Vous pouvez personnaliser les paramètres de mémoire tampon utilisés dans un point de capture, en particulier la taille de la mémoire tampon et le mode de mémoire tampon.

- La taille minimale de la mémoire tampon est de 1 Mo et la taille maximale est de 20 Mo.

- Si aucune taille de mémoire tampon n'est spécifiée, une taille par défaut de 5 Mo sera utilisée.
- Un maximum de 20 Mo de mémoire peut être alloué à tous les points de capture. Un seul point de capture peut se voir allouer 20 Mo, mais vous ne pouvez pas avoir quatre points de capture configurés chacun pour utiliser 20 Mo. Le total de 20 Mo est réparti entre tous les points de capture configurés.
- Il existe deux modes de tampon : linéaire et circulaire.
- Le mode linéaire est le mode par défaut. En mode linéaire, une capture de paquets active collecte les données jusqu'à ce que le tampon configuré soit plein, puis la capture s'arrête. En outre, vous ne pourrez pas redémarrer une capture de paquets lors de l'utilisation de la journalisation linéaire et si la mémoire tampon est déjà pleine. Dans ce cas, vous devez d'abord effacer la mémoire tampon.
- En mode tampon circulaire, une fois la mémoire tampon pleine, elle écrasera les données précédemment capturées à l'aide de la fonction FIFO (First In First Out). Une capture utilisant le mode tampon circulaire doit être arrêtée manuellement.

Étape 1

La commande permettant de configurer manuellement les paramètres de la mémoire tampon est `monitor capture {capture-name} buffer {circulaire [size buffer-size] | size buffer-size}`.

```
monitor capture cap1 buffer size 2 circular
```

Dans cet exemple, une taille de mémoire tampon de 2 Mo est configurée pour le point de capture cap1 et le mode de mémoire tampon est circulaire.

```
switch4acl2e#monitor capture cap1 buffer size 2 circular
switch4acl2e#show monitor capture cap1

Status Information for Capture cap1
  Target Type:
  Interface: None, Direction: NONE
  Status : Inactive
  Filter Details:
  None
  Buffer Details:
  Buffer Type: CIRCULAR
  Buffer size (in MB): 2
switch4acl2e#
```

Étape 2

Utilisation de la commande `no monitor capture {capture-name} buffer {circulaire [size buffer-size] | size buffer-size}` rétablira le mode de mémoire tampon au mode linéaire

par défaut.

```
no monitor capture cap1 buffer size 2 circular
```

Note:

L'utilisation de la commande « no » sans les options [circulaire] et [size] permet de définir le mode et la taille de la mémoire tampon sur leur paramètre par défaut, à savoir le mode linéaire et la taille de la mémoire tampon de 5 Mo.

Étape 3

Pour vider une mémoire tampon, utilisez la commande `monitor capture {capture-name} clear`.

```
monitor capture cap1 clear
```

Dans cet exemple, la mémoire tampon de cap1 utilisait 256 Ko. Après l'exécution de la commande `clear`, la mémoire tampon est maintenant à 0 Ko.

```
switch4acl2e#show monitor capture cap1 buffer
buffer size (KB)           : 5120
buffer used (KB)           : 256
packets in buf             : 841
packets dropped            : 0
Packet rate per second    : 0
switch4acl2e#monitor capture cap1 clear
Captured data will be deleted [clear]? (Y/N) [Y] Y
Cleared capture point : cap1
switch4acl2e#show monitor capture cap1 buffer
buffer size (KB)           : 5120
buffer used (KB)           : 0
packets in buf             : 0
packets dropped            : 0
Packet rate per second    : 0
switch4acl2e#
```

Paramètres d'interface source

Une fois qu'un point de capture a été créé, l'interface source de la capture doit être

définie. Le paramètre de l'interface source est obligatoire pour démarrer une capture.

- Actuellement, le plan de contrôle est le seul type de source pris en charge.
- Pour définir la direction, choisissez l'une des options suivantes : entrée, sortie ou les deux.
- Entrée : capture les paquets entrants vers le commutateur.
- Sortant : capture les paquets sortants du commutateur.
- Both : capture les paquets entrants et sortants.

Étape 1

Utilisez la commande `monitor capture {capture-name} control-plane {in | dehors | both}` pour configurer le paramètre de l'interface source.

```
monitor capture cap1 control-plane both
```

```
switch4acl2e#monitor capture cap1 control-plane both
switch4acl2e#show monitor capture cap1

Status Information for Capture cap1
  Target Type:
  Interface: Control Plane, Direction: BOTH
  Status : Inactive
  Filter Details:
  None
  Buffer Details:
  Buffer Type: CIRCULAR
  Buffer size (in MB): 2
switch4acl2e#
```

Étape 2

Utilisez le plan de contrôle `no monitor capture {capture-name} {in | dehors | both}` pour supprimer le paramètre d'interface source.

```
no monitor capture cap1 control-plane both
```

Capter les paramètres de filtre

Le filtre de capture est un paramètre obligatoire qui doit être configuré pour une capture de paquets. Actuellement, le fonctionnement du filtre n'est pas pris en charge dans le microprogramme 4.1.3.36. et tous les paquets sur l'interface source (qui est le plan de contrôle) seront capturés. Cependant, vous devrez toujours configurer ce

paramètre à l'aide de l'option « any ».

Utilisez la commande `monitor capture {capture-name} match any` pour configurer le paramètre du filtre de capture.

```
monitor capture cap1 match any
```

Dans cet exemple, le point de capture `cap1` a été configuré pour correspondre à tous les paquets.

```
switch4ac12e#monitor capture cap1 match any
switch4ac12e#show monitor capture cap1

Status Information for Capture cap1
  Target Type:
  Interface: Control Plane, Direction: BOTH
  Status : Inactive
  Filter Details:
    Capture all packets
  Buffer Details:
    Buffer Type: LINEAR (default)
    Buffer size (in MB): 5 (default)
switch4ac12e#
```

Démarrage et arrêt de la capture

Avant de commencer une capture, assurez-vous de :

- Définissez l'interface source et le filtre de capture.
- Il est recommandé de vérifier l'utilisation du processeur avant de commencer.

Il est important de noter qu'une seule session de capture peut être active à la fois. Si une capture est redémarrée après avoir été arrêtée, les nouveaux paquets sont ajoutés à la mémoire tampon. Cependant, une capture ne peut pas être redémarrée si la mémoire tampon est pleine et que le mode est défini sur linéaire.

Étape 1

Pour démarrer la capture, utilisez la commande `monitor capture {capture-name} start`.

```
monitor capture cap1 start
```

Étape 2

Pour arrêter une capture, utilisez la commande `monitor capture {capture-name} stop`.

```
monitor capture cap1 stop
```

```
switch4ac12e#monitor capture cap1 start
Started capture point : cap1
switch4ac12e#monitor capture cap1 stop
Stopped capture point : cap1
switch4ac12e#
```

Enregistrement des données de capture de paquets

Une fois la capture de paquets terminée, les données de la mémoire tampon (qui est de la mémoire vive) doivent être enregistrées. Il existe deux cas où les données sont enregistrées :

- Déclenché par un utilisateur à l'aide d'une commande CLI
- Automatiquement si une erreur fatale se produit.

Un utilisateur peut enregistrer la capture de paquets dans la mémoire flash intégrée du commutateur, s'il y a de l'espace pour celle-ci, ou sur un périphérique USB connecté tel qu'un lecteur flash. Si une erreur fatale se produit pendant une capture de paquets, les données sont automatiquement enregistrées dans le répertoire principal de la mémoire flash.

Pour exporter la capture de paquets, utilisez la commande `monitor capture {capture-name} export {destination/filename}`

```
monitor capture cap1 export flash: cap1.pcap
```

```
monitor capture cap1 export usb: cap1.pcap
```

```
switch4acl2e#monitor capture capl export flash:capl.pcap
Copy: 270862 bytes copied in 00:00:01 [hh:mm:ss]
switch4acl2e#monitor capture capl export usb:capl.pcap
Copy: 270862 bytes copied in 00:00:01 [hh:mm:ss]
switch4acl2e#
```

Si une capture est enregistrée dans la mémoire flash, elle peut être copiée sur un lecteur flash USB via la commande CLI `copy {filename} usb:/`

Les commutateurs C1200 et C1300 prennent en charge les lecteurs USB formatés en FAT et FAT32. Si vous ne disposez pas d'un lecteur FAT ou FAT32 USB, vous devrez copier le fichier à partir du commutateur à l'aide du protocole TFTP.

Pour copier un fichier du commutateur à l'aide du protocole TFTP :

- Configurer un serveur TFTP (à l'aide de TFTP64 ou d'un autre service)
- Utilisez la commande suivante à partir de l'interface de ligne de commande du commutateur :
`copy flash: {pcap file name} tftp://{tftp server ip}/{pcap file name}`

Conclusion

Vous connaissez maintenant la fonction de capture de paquets intégrée dans les commutateurs Catalyst 1200 et 1300 et les commandes CLI permettant de configurer les paramètres.

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.