Dépannage des problèmes DHCP sur les agents de relais DHCP du Catalyst 9000

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Produits connexes
- Informations générales
- Problème
  - Scénario 1 : redirections ICMP
    - Solution
  - Scénario 2 : ICMP inaccessible
    - Solution
  - Scénario 3 : ICMP TTL-Exceeded
    - Solution
- Informations connexes

Introduction

Ce document décrit comment dépanner les échecs d'allocation d'adresses DHCP lents ou intermittents sur les commutateurs Catalyst 9000 en tant qu'agents de relais DHCP.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- DHCP (Dynamic Host Configuration Protocol) et agents de relais DHCP
- Internet Control Message Protocol (ICMP)
- Contrôle du plan de contrôle (CoPP)

Composants utilisés

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

- Commutateurs de la gamme Catalyst 9000
- Cisco IOS® XE versions 16.x et 17.x

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.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Commutateurs de la gamme Catalyst 3650/3850 avec Cisco IOS XE 16.x

Informations générales

Ce document décrit comment dépanner les défaillances lentes d'allocation d'adresses DHCP (Dynamic Host Configuration Protocol) ou intermittentes sur les commutateurs de la gamme Catalyst 9000 en tant qu'agents de relais DHCP.

La fonctionnalité Control Plane Policing (CoPP) améliore la sécurité de votre périphérique en protégeant le processeur contre le trafic inutile et les attaques par déni de service (DoS). Il peut également protéger le trafic de contrôle et le trafic de gestion contre les pertes de trafic causées par des volumes élevés d'autres trafics de moindre priorité.

Votre périphérique est généralement segmenté en trois plans de fonctionnement, chacun ayant son propre objectif :

- Le plan de données, pour transférer des paquets de données.
- Le plan de contrôle, pour acheminer les données correctement.
- Le plan de gestion, pour gérer les éléments du réseau.

Vous pouvez utiliser le protocole CoPP pour protéger la plupart du trafic lié au processeur et assurer la stabilité du routage, l'accessibilité et la livraison des paquets. Plus important encore, vous pouvez utiliser CoPP pour protéger le processeur d'une attaque DoS.

CoPP utilise l'interface de ligne de commande (MQC) QoS modulaire et les files d'attente CPU pour atteindre ces objectifs. Différents types de trafic du plan de contrôle sont regroupés en fonction de certains critères et affectés à une file d'attente du processeur. Vous pouvez gérer ces files d'attente de CPU en configurant des contrôleurs dédiés dans le matériel. Par exemple, vous pouvez modifier le débit du régulateur pour certaines files d'attente de CPU (type de trafic), ou vous pouvez désactiver le régulateur pour un certain type de trafic.

Bien que les contrôleurs soient configurés dans le matériel, le protocole CoPP n'affecte pas les performances du processeur ni celles du plan de données. Mais comme il limite le nombre de paquets dirigés vers le CPU, la charge du CPU est contrôlée. Cela signifie que les services qui attendent des paquets du matériel peuvent voir un taux plus contrôlé de paquets entrants (le taux est configurable par l'utilisateur).

Problème

Un commutateur Catalyst 9000 est configuré en tant qu'agent de relais DHCP lorsque la commande ip helper-address est configurée sur une interface routée ou une interface SVI. L'interface sur laquelle l'adresse d'assistance est configurée est généralement la passerelle par défaut pour les clients en aval. Pour que le commutateur puisse fournir des services de relais DHCP à ses clients, il doit être en mesure de traiter les messages de détection DHCP entrants. Cela nécessite que le commutateur reçoive la détection DHCP et envoie ce paquet à son processeur pour qu'il soit traité. Une fois la détection DHCP reçue et traitée, l'agent de relais crée un nouveau paquet de monodiffusion provenant de l'interface où la détection DHCP a été reçue et destiné à l'adresse IP telle que définie dans la configuration ip helper-address. Une fois le paquet créé, il est transféré par le matériel et envoyé au serveur DHCP où il peut être traité et finalement renvoyé à l'agent de relais afin que le processus DHCP puisse continuer pour le client.

Un problème courant se produit lorsque des paquets de transaction DHCP au niveau de l'agent de relais sont affectés par inadvertance par le trafic qui est envoyé au CPU parce qu'il est soumis à un scénario ICMP spécifique, tel qu'une redirection ICMP ou un message ICMP Destination Unreachable. Ce comportement peut se manifester par le fait que les clients ne peuvent pas obtenir une adresse IP de DHCP en temps voulu, ou même par un échec total d'attribution DHCP. Dans certains scénarios, le comportement ne peut être observé qu'à certains moments de la journée, par exemple pendant les heures de pointe, lorsque la charge sur le réseau est entièrement maximisée.

Comme indiqué dans la section Arrière-plan, les commutateurs de la gamme Catalyst 9000 sont livrés avec une stratégie CoPP par défaut configurée et activée sur le périphérique. Cette politique CoPP agit comme une politique de qualité de service (QoS) qui se trouve sur le chemin du trafic qui est reçu sur les ports du panneau avant et qui est destiné au CPU du périphérique. Il limite le trafic en fonction du type de trafic et des seuils prédéfinis configurés dans la stratégie. Les paquets de contrôle de routage (généralement marqués avec DSCP CS6), les paquets de contrôle de topologie (BPDU STP) et les paquets à faible latence (BFD) sont des exemples de trafic classifié et limité par défaut. Ces paquets doivent être classés par ordre de priorité, car la capacité à les traiter de manière fiable permet d'obtenir un environnement réseau stable.

Affichez les statistiques du régulateur CoPP avec la commande show platform hardware fed switch active qos queue stats internal cpu policer.

La file d'attente de redirection ICMP (file d'attente 6) et la file d'attente BROADCAST (file d'attente 12) partagent le même PlcIdx de 0 (index du contrôleur). Cela signifie que tout trafic de diffusion qui doit être traité par le processeur du périphérique, tel qu'une détection DHCP, est partagé avec le trafic qui est également destiné au processeur du périphérique dans la file d'attente de redirection ICMP. Cela peut entraîner le problème mentionné précédemment où les transactions DHCP échouent parce que le trafic de la file d'attente de redirection ICMP prive le trafic qui doit être traité par la file d'attente de DIFFUSION, ce qui entraîne l'abandon de paquets de diffusion légitimes.

<#root>

```
9300-Switch#
```

```
show platform hardware fed switch active qos queue stats internal cpu policer
```

```
                        CPU Queue Statistics
============================================================================================
                                                (default) (set)     Queue        Queue
QId PlcIdx  Queue Name                 Enabled   Rate     Rate      Drop(Bytes)  Drop(Frames)
--------------------------------------------------------------------------------------------
0    11     DOT1X Auth                  Yes     1000      1000     0            0
1    1      L2 Control                  Yes     2000      2000     0            0
2    14     Forus traffic               Yes     4000      4000     0            0
3    0      ICMP GEN                    Yes     600       600      0            0
4    2      Routing Control             Yes     5400      5400     0            0
5    14     Forus Address resolution    Yes     4000      4000     0            0

6    0      ICMP Redirect               Yes     600       600      0            0  <-- Policer Index 0


7    16     Inter FED Traffic           Yes     2000      2000     0            0
8    4      L2 LVX Cont Pack            Yes     1000      1000     0            0
9    19     EWLC Control                Yes     13000     13000    0            0
10   16     EWLC Data                   Yes     2000      2000     0            0
11   13     L2 LVX Data Pack            Yes     1000      1000     0            0

12   0      BROADCAST                   Yes     600       600      0            0  <-- Policer Index 0


13   10     Openflow                    Yes     200       200      0            0
14   13     Sw forwarding               Yes     1000      1000     0            0
15   8      Topology Control            Yes     13000     16000    0            0
16   12     Proto Snooping              Yes     2000      2000     0            0
17   6      DHCP Snooping               Yes     500       500      0            0
18   13     Transit Traffic             Yes     1000      1000     0            0
19   10     RPF Failed                  Yes     250       250      0            0
20   15     MCAST END STATION           Yes     2000      2000     0            0
<snip>
```

Le trafic qui dépasse le débit de 600 paquets par seconde par défaut dans la stratégie CoPP est abandonné avant d'atteindre le processeur.

<#root>

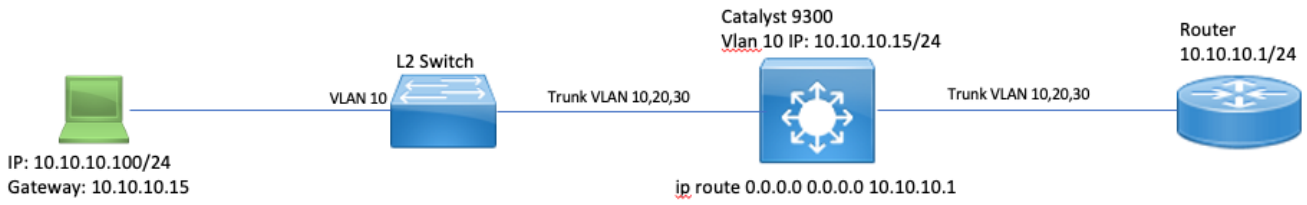
```
9300-Switch#

show platform hardware fed switch active qos queue stats internal cpu policer
```

```
                        CPU Queue Statistics
============================================================================================
                                                (default) (set)     Queue        Queue
QId PlcIdx  Queue Name                 Enabled   Rate     Rate      Drop(Bytes)  Drop(Frames)
--------------------------------------------------------------------------------------------
0    11     DOT1X Auth                  Yes     1000      1000     0            0
1    1      L2 Control                  Yes     2000      2000     0            0
2    14     Forus traffic               Yes     4000      4000     0            0
3    0      ICMP GEN                    Yes     600       600      0            0
4    2      Routing Control             Yes     5400      5400     0            0
5    14     Forus Address resolution    Yes     4000      4000     0            0

6    0      ICMP Redirect               Yes     600       600      3063106173577 3925209161    <-- Dropp
```

```
7     16      Inter FED Traffic           Yes     2000      2000      0             0
8     4       L2 LVX Cont Pack            Yes     1000      1000      0             0
9     19      EWLC Control                Yes     13000     13000     0             0
10    16      EWLC Data                   Yes     2000      2000      0             0
11    13      L2 LVX Data Pack            Yes     1000      1000      0             0

12    0       BROADCAST                   Yes     600       600       1082560387 3133323          <-- Dropp

13    10      Openflow                    Yes     200       200       0             0
14    13      Sw forwarding               Yes     1000      1000      0             0
15    8       Topology Control            Yes     13000     16000     0             0
16    12      Proto Snooping              Yes     2000      2000      0             0
17    6       DHCP Snooping               Yes     500       500       0             0
18    13      Transit Traffic             Yes     1000      1000      0             0
19    10      RPF Failed                  Yes     250       250       0             0
20    15      MCAST END STATION           Yes     2000      2000      0             0
<snip>
```

Scénario 1 : redirections ICMP

Considérez cette topologie pour le premier scénario :



La séquence des événements est la suivante :

1. Un utilisateur sur 10.10.10.100 établit une connexion Telnet avec le périphérique 10.100.100.100, un réseau distant.

2. L'adresse IP de destination se trouve dans un sous-réseau différent. Le paquet est donc envoyé à la passerelle par défaut des utilisateurs, 10.10.10.15.

3. Lorsque le Catalyst 9300 reçoit ce paquet pour le router, il envoie le paquet à son processeur pour générer une redirection ICMP.

La redirection ICMP est générée parce que du point de vue du commutateur 9300, il serait plus efficace pour l'ordinateur portable d'envoyer simplement ce paquet au routeur à l'adresse 10.10.10.1 directement, puisque c'est le prochain saut de Catalyst 9300 de toute façon, et il est dans le même VLAN que l'utilisateur est dans.

Le problème est que le flux entier est traité au niveau du processeur, car il répond aux critères de redirection ICMP. Si d'autres périphériques envoient du trafic qui répond au scénario de redirection ICMP, encore plus de trafic commence à être envoyé au CPU dans cette file d'attente, ce qui pourrait avoir un impact sur la file d'attente BROADCAST puisqu'ils partagent le même

contrôleur CoPP.

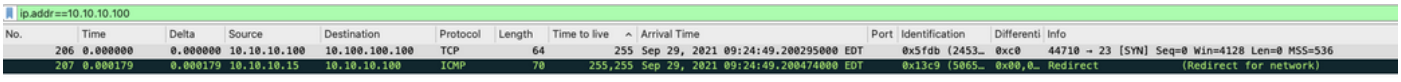
Debug ICMP pour afficher le syslog ICMP Redirect.

<#root>

```
9300-Switch#

debug ip icmp       <-- enables ICMP debugs


ICMP packet debugging is on
9300-Switch#

show logging | inc ICMP


*Sep 29 12:41:33.217: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE, dscp 0 t
*Sep 29 12:41:33.218: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE, dscp 0 t
*Sep 29 12:41:33.219: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE, dscp 0 t
*Sep 29 12:41:33.219: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE, dscp 0 t
*Sep 29 12:43:08.127: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw 10.10.10.1
*Sep 29 12:50:09.517: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw 10.10.10.1

*Sep 29 12:50:10.017: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw 10.10.10.1


*Sep 29 12:50:14.293: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw 10.10.10.1
*Sep 29 12:50:19.053: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw 10.10.10.1
*Sep 29 12:50:23.797: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw 10.10.10.1
*Sep 29 12:50:28.537: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw 10.10.10.1
*Sep 29 12:50:33.284: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw 10.10.10.1
```

⚠ Attention : en raison du niveau de détail à l'échelle, il est recommandé de désactiver la journalisation de la console et la surveillance du terminal avant d'activer les débogages ICMP.

Une capture de paquets intégrée au niveau du processeur Catalyst 9300 affiche le SYN TCP initial pour la connexion Telnet au niveau du processeur ainsi que la redirection ICMP générée.



Le paquet de redirection ICMP provient de l'interface VLAN 10 du Catalyst 9300 et est destiné au client. Il contient les en-têtes de paquet d'origine pour lesquels le paquet de redirection ICMP est envoyé.

```
▼ Internet Protocol Version 4, Src: 10.10.10.15, Dst: 10.10.10.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x13c9 (5065)
  ▶ Flags: 0x0000
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x7f75 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.15
    Destination: 10.10.10.100
▼ Internet Control Message Protocol
    Type: 5 (Redirect)
    Code: 0 (Redirect for network)
    Checksum: 0x2bec [correct]
    [Checksum Status: Good]
    Gateway address: 10.10.10.1
  ▼ Internet Protocol Version 4, Src: 10.10.10.100, Dst: 10.100.100.100
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
      Total Length: 44
      Identification: 0x5fdb (24539)
    ▶ Flags: 0x0000
      Time to live: 255
      Protocol: TCP (6)
      Header checksum: 0xd7fa [validation disabled]
      [Header checksum status: Unverified]
      Source: 10.10.10.100
      Destination: 10.100.100.100
  ▶ Transmission Control Protocol, Src Port: 44710, Dst Port: 23
```

Solution

Dans ce scénario, les paquets qui sont envoyés au CPU peuvent être évités, ce qui arrête également la génération du paquet de redirection ICMP.

Les systèmes d'exploitation modernes n'utilisent pas les messages de redirection ICMP, de sorte que les ressources requises pour générer, envoyer et traiter ces paquets ne constituent pas une utilisation efficace des ressources CPU sur les périphériques réseau.

Vous pouvez également indiquer à l'utilisateur d'utiliser la passerelle par défaut 10.10.10.1, mais une telle configuration peut être en place pour une raison quelconque et n'entre pas dans le cadre de ce document.

Désactivez simplement les redirections ICMP avec la commande no ip redirects CLI.

<#root>

```
9300-Switch#
```

```
conf t


Enter configuration commands, one per line. End with CNTL/Z.
9300-Switch(config)#
interface vlan 1

0
9300-Switch(config-if)#
no ip redirects       <-- disable IP redirects


9300-Switch(config-if)#end
```

Vérifiez que les redirections ICMP sont désactivées sur une interface.

<#root>

```
9300-Switch#
show ip interface vlan 10


 Vlan10 is up, line protocol is up
 Internet address is 10.10.10.15/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.102
 Outgoing Common access list is not set
 Outgoing access list is not set
 Inbound Common access list is not set
 Inbound access list is BLOCK-TELNET
 Proxy ARP is disabled
 Local Proxy ARP is disabled
 Security level is default
 Split horizon is enabled


ICMP redirects are never sent       <-- redirects disabled


 ICMP unreachables are never sent
 ICMP mask replies are never sent
 IP fast switching is enabled
 IP Flow switching is disabled
 IP CEF switching is enabled
 IP CEF switching turbo vector
 <snip>
```

Pour plus d'informations sur les redirections ICMP et le moment où elles sont envoyées, consultez le lien suivant : https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-43.html

Scénario 2 : ICMP inaccessible

Considérez la même topologie où l'utilisateur à l'adresse 10.10.10.100 établit une connexion Telnet à l'adresse 10.100.100.100. Cette fois, une liste d'accès a été configurée en entrée sur l'interface SVI du VLAN 10 qui bloque les connexions Telnet.

<#root>

```
9300-Switch#
```

show running-config interface vlan 10

```
Building Configuration..

Current Configuration : 491 bytes
!
interface Vlan10
 ip address 10.10.10.15 255.255.255.0
 no ip proxy-arp
```

ip access-group BLOCK-TELNET in <-- inbound ACL

```
end

9300-Switch#

9300-Switch#
```

show ip access-list BLOCK-TELNET

```
Extended IP access list BLOCK-TELNET
```

10 deny tcp any any eq telnet <-- block telnet

```
    20 permit ip any any
9300-Switch#
```

La séquence des événements est la suivante :

1. L’utilisateur à l’adresse 10.10.10.100 établit une connexion Telnet avec le périphérique 10.100.100.100.

2. L’adresse IP de destination se trouve dans un sous-réseau différent. Le paquet est donc envoyé à la passerelle par défaut des utilisateurs.

3. Lorsque le Catalyst 9300 reçoit ce paquet, il est évalué par rapport à la liste de contrôle d’accès entrante et il est bloqué.

4. Comme le paquet est bloqué et que les adresses IP inaccessibles sont activées sur l’interface, le paquet est envoyé au processeur afin que le périphérique puisse générer un paquet ICMP de destination inaccessible.

Déboguez ICMP pour afficher le syslog ICMP de destination inaccessible.

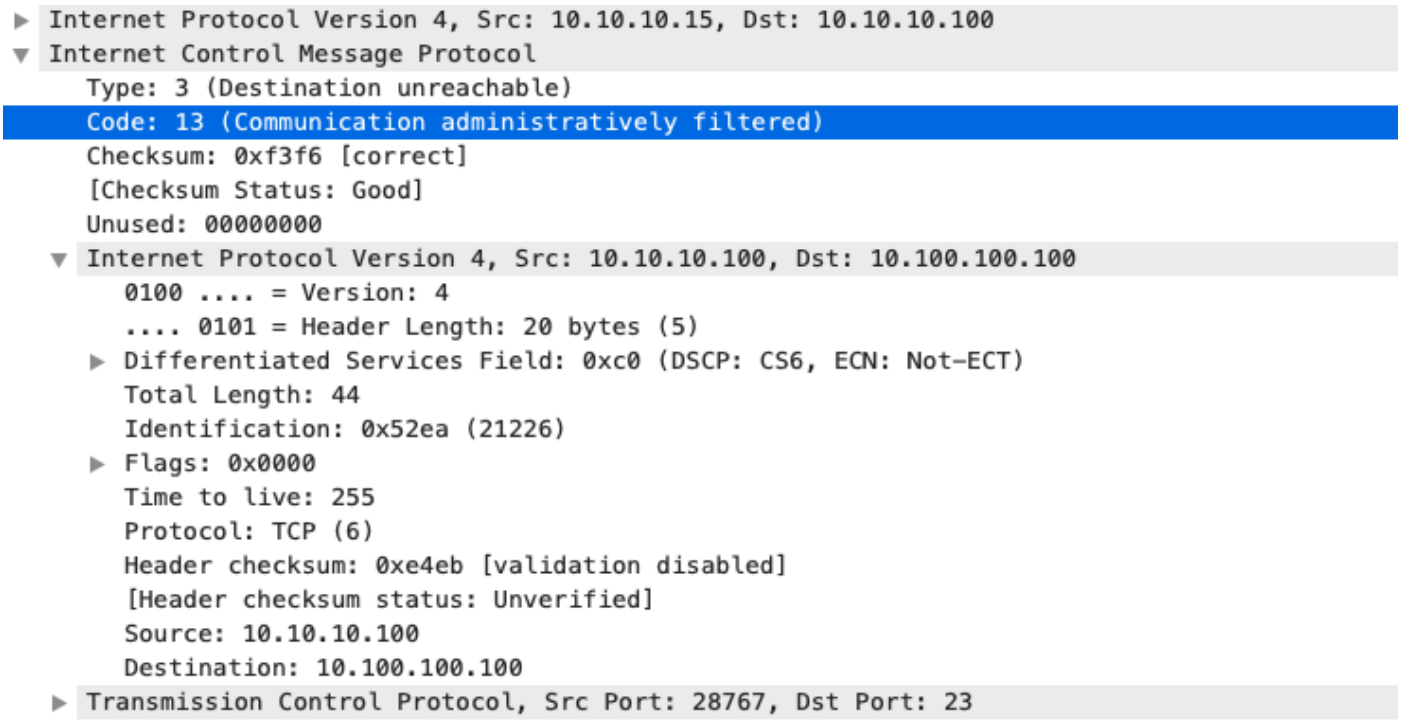
<#root>

```
9300-Switch#
debug ip icmp              <-- enables ICMP debugs

ICMP packet debugging is on
9300-Switch#
show logging | include ICMP

<snip>
*Sep 29 14:01:29.041: ICMP: dst (10.100.100.100) administratively prohibited unreachable sent to 10.10.1
```

⚠ Attention : en raison du niveau de détail à l'échelle, il est recommandé de désactiver la journalisation de la console et la surveillance du terminal avant d'activer les débogages ICMP.

Une capture de paquets intégrée au niveau du processeur Catalyst 9300 affiche le SYN TCP initial pour la connexion Telnet au niveau du processeur ainsi que la destination ICMP inaccessible qui est envoyée.

Le paquet ICMP Destination Unreachable provient de l’interface VLAN 10 du Catalyst 9300 et est destiné au client. Il contient les en-têtes de paquet d’origine pour lesquels le paquet ICMP est envoyé.



Solution

Dans ce scénario, désactivez le comportement où les paquets renvoyés sont bloqués par une liste de contrôle d'accès afin de générer le message ICMP Destination Unreachable (Destination inaccessible).

La fonctionnalité IP Unreachable est activée par défaut sur les interfaces routées des commutateurs de la gamme Catalyst 9000.

<#root>

```
9300-Switch#
```

configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
9300-Switch(config)#
```

interface vlan 10

```
9300-Switch(config-if)#
```

no ip unreachables   <-- disable IP unreachables

Vérifiez qu'elles sont désactivées pour l'interface.

<#root>

```
9300-Switch#
```

`show ip interface vlan 10`

```
 Vlan10 is up, line protocol is up
 Internet address is 10.10.10.15/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.102
 Outgoing Common access list is not set
 Outgoing access list is not set
 Inbound Common access list is not set
 Inbound access list is BLOCK-TELNET
 Proxy ARP is disabled
 Local Proxy ARP is disabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are never sent
```

`ICMP unreachables are never sent     <-- IP unreachables disabled`

```
 ICMP mask replies are never sent
 IP fast switching is enabled
 IP Flow switching is disabled
 IP CEF switching is enabled
 IP CEF switching turbo vector
 <snip>
```

Scénario 3 : ICMP TTL-Exceeded

Considérez la topologie précédente utilisée pour les deux scénarios précédents. Cette fois, l'utilisateur sur 10.10.10.100 tente d'atteindre une ressource dans un réseau qui a été mis hors service depuis. De ce fait, les interfaces SVI et VLAN qui hébergeaient ce réseau n'existent plus sur le Catalyst 9300. Cependant, le routeur a toujours une route statique qui pointe vers l'interface VLAN 10 du Catalyst 9300 comme tronçon suivant pour ce réseau.

Comme ce réseau n’est plus configuré sur le Catalyst 9300, il n’est pas affiché comme connecté directement et le Catalyst 9300 achemine tous les paquets pour lesquels il n’a pas de route spécifique vers sa route statique par défaut qui pointe vers le routeur à l’adresse 10.10.10.1.

Ce comportement introduit une boucle de routage dans le réseau lorsque l'utilisateur tente de se connecter à une ressource dans l'espace d'adressage 192.168.10.0/24. Le paquet est bouclé entre le routeur 9300 et le routeur jusqu'à l'expiration de la durée de vie.

1. L'utilisateur tente de se connecter à une ressource du réseau 192.168.10/24

2. Le paquet est reçu par Catalyst 9300 et est routé vers sa route par défaut avec le saut suivant 10.10.10.1 et décrémente la durée de vie de 1.

3. Le routeur reçoit ce paquet et vérifie la table de routage pour trouver une route pour ce réseau avec le tronçon suivant 10.10.10.15. Il décrémente la durée de vie de 1 et réachemine le paquet vers le routeur 9300.

4. Catalyst 9300 reçoit le paquet et le réachemine à nouveau vers 10.10.10.1 et décrémente la durée de vie de 1.

Ce processus se répète jusqu'à ce que la durée de vie IP atteigne zéro.

Lorsque le Catalyst reçoit le paquet avec IP TTL = 1, il envoie le paquet au CPU et génère un message ICMP TTL-Exceeded (Dépassement de la durée de vie).

Le type de paquet ICMP est 11 avec le code 0 (durée de vie expirée pendant le transit). Ce type de paquet ne peut pas être désactivé via les commandes CLI

Le problème avec le trafic DHCP entre en jeu dans ce scénario parce que les paquets qui sont en boucle sont soumis à la redirection ICMP car ils laissent de côté la même interface sur laquelle ils ont été reçus.

Les paquets envoyés par l'utilisateur sont également soumis à une redirection ICMP. Dans ce scénario, le trafic DHCP peut facilement être affamé de la file d'attente BROADCAST. À grande échelle, ce scénario serait encore pire en raison du nombre de paquets placés dans la file d'attente de redirection.

Ici, les abandons CoPP sont démontrés via 1000 requêtes ping vers le réseau 192.168.10.0/24 avec un délai d'attente de 0 seconde entre chaque requête ping. Les statistiques CoPP sur le 9300 sont effacées et à zéro octet abandonné avant l'envoi des requêtes ping.

<#root>

```
9300-Switch#

clear platform hardware fed switch active qos statistics internal cpu policer                    <-- cl


9300-Switch#

show platform hardware fed switch active qos queue stats internal cpu policer | i Redirect|Drop   <-- ve
```

```
QId PlcIdx  Queue Name                Enabled   Rate     Rate        Drop(Bytes)     Drop(Frames)
6    0      ICMP Redirect              Yes     600       600

0               0                          <-- bytes dropped 0

<snip>
```

L'utilisateur envoie le trafic au réseau distant.

```
<#root>

User#

ping 192.168.10.10 timeout 0 rep 1000   <-- User sends 1000 pings


Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.10.10, timeout is 0 seconds:
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................
Success rate is 0 percent (0/1000)
```

Les débogages ICMP affichent les journaux système Redirect et TTL-Exceeded dus à la boucle de routage.

```
<#root>

9300-Switch#

debug ip icmp


ICMP packet deubgging is on
*Sep 29 16:33:22.676: ICMP:

redirect sent to 10.10.10.100 for dest 192.168.10.10, use gw 10.10.10.1    <-- redirect sent


*Sep 29 16:33:22.678: ICMP:

time exceeded (time to live) sent to 10.10.10.100 (dest was 192.168.10.10), topology BASE, dscp 0 topoid
```

```
*Sep 29 16:33:22.678: ICMP: time exceeded (time to live) sent to 10.10.10.100 (dest was 192.168.10.10),
*Sep 29 16:33:22.678: ICMP: time exceeded (time to live) sent to 10.10.10.100 (dest was 192.168.10.10),
<snip>
```

⚠ Attention : en raison du niveau de détail à l'échelle, il est recommandé de désactiver la journalisation de la console et la surveillance du terminal avant d'activer les débogages ICMP.

Les abandons CoPP sont visibles en raison de la quantité de trafic envoyée au CPU pour la redirection. Notez que ceci est seulement pour un client unique.

<#root>

9300-Switch#

show platform hardware fed switch active qos queue stats internal cpu policer

```
                          CPU Queue Statistics
============================================================================================
                                                  (default) (set)     Queue         Queue
QId PlcIdx  Queue Name                 Enabled    Rate      Rate      Drop(Bytes)   Drop(Frames)
--------------------------------------------------------------------------------------------
0    11     DOT1X Auth                   Yes      1000      1000      0             0
1    1      L2 Control                   Yes      2000      2000      0             0
2    14     Forus traffic                Yes      4000      4000      0             0
3    0      ICMP GEN                     Yes      600       600       0             0
4    2      Routing Control              Yes      5400      5400      0             0
5    14     Forus Address resolution     Yes      4000      4000      0             0

6    0      ICMP Redirect                Yes      600       600       15407990      126295    <-- drops in r


7    16     Inter FED Traffic            Yes      2000      2000      0             0
8    4      L2 LVX Cont Pack             Yes      1000      1000      0             0
<snip>
```

Solution

Dans ce scénario, la solution consiste à désactiver les redirections ICMP, comme dans le scénario 1. La boucle de routage est également un problème, mais l'intensité est aggravée car les paquets sont également dirigés pour la redirection.

Les paquets ICMP TTL-Exceeded sont également renvoyés lorsque TTL est égal à 1, mais ces paquets utilisent un index CoPP Policer différent et ne partagent pas de file d'attente avec BROADCAST, de sorte que le trafic DHCP n'est pas affecté.

Désactivez simplement les redirections ICMP avec la CLI no ip redirects.

<#root>

```
9300-Switch#
configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
9300-Switch(config)#
interface vlan 10

9300-Switch(config-if)#
no ip redirects        <-- disable IP redirects

9300-Switch(config-if)#
end
```

Informations connexes

- Configuration de la capture de paquets intégrée
- Présentation des redirections ICMP
- Assistance et documentation techniques - Cisco Systems

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.