Comprendre les messages de redirection ICMP

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Messages de redirection ICMP

Chemins sous-optimaux via les réseaux Ethernet

- Routage statique
- Policy-based routing

Redirections ICMP sur des liaisons point à point

Considérations relatives à Nexus Platform

Outils de surveillance et de diagnostic du trafic

- show ip traffic
- Ethanalyseur

Désactiver les redirections ICMP

Résumé

Introduction

Ce document décrit la fonctionnalité de redirection de paquets ICMP (Internet Control Message Protocol).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Architecture de plate-forme Nexus 7000
- Configuration du logiciel Cisco NX-OS
- Protocole RFC (Internet Control Message Protocol), tel que décrit dans le document RFC 792

Composants utilisés

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

- Nexus 7000

- Logiciel Cisco NX-OS

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.

Informations générales

Ce document traite de la fonctionnalité de redirection de paquets fournie par le protocole ICMP (Internet Control Message Protocol). Le document explique ce que la présence de messages de redirection ICMP dans le réseau indique habituellement, et ce qui peut être fait pour minimiser les effets secondaires négatifs associés aux conditions du réseau qui causent la génération de messages de redirection ICMP.

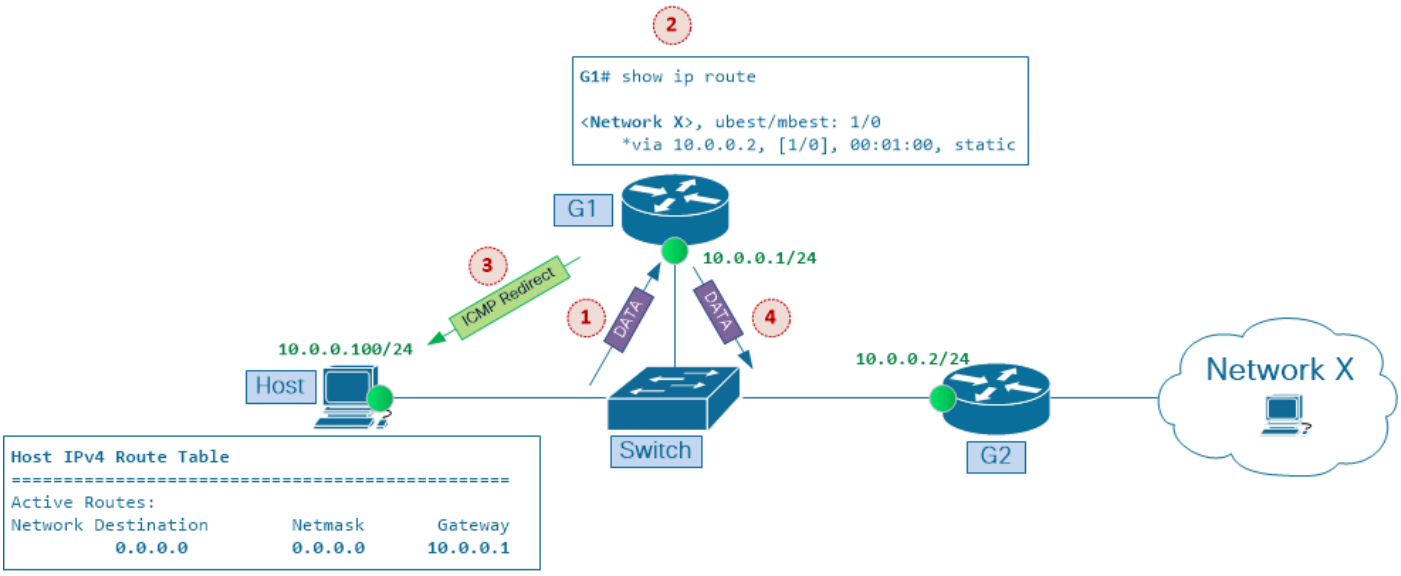
Messages de redirection ICMP

La fonctionnalité de redirection ICMP est expliquée dans le RFC 792 Internet Control Message Protocol avec cet exemple :

> Dans ce cas, la passerelle envoie un message de redirection à un hôte.
>
> Une passerelle, G1, reçoit un datagramme Internet d'un hôte sur un réseau auquel la passerelle est connectée. La passerelle, G1, vérifie sa table de routage et obtient l'adresse de la passerelle suivante, G2, sur la route vers le réseau de destination Internet du datagramme, X
>
> Si G2 et l'hôte identifié par l'adresse source Internet du datagramme se trouvent sur le même réseau, un message de redirection est envoyé à l'hôte. Le message de redirection conseille à l'hôte d'envoyer son trafic pour le réseau X directement à la passerelle G2, car il s'agit d'un chemin plus court vers la destination.
>
> La passerelle transmet les données de datagramme d'origine à sa destination Internet.

Ce scénario est illustré dans l'image 1. L'hôte et deux routeurs, G1 et G2, sont connectés à un segment Ethernet partagé et possèdent des adresses IP sur le même réseau 10.0.0.0/24

Image1 - Redirections ICMP dans des réseaux Ethernet multipoints



Redirections ICMP dans des réseaux Ethernet multipoints

L'hôte a l'adresse IP 10.0.0.100. La table de routage de l'hôte comporte une entrée de route par défaut qui pointe vers l'adresse IP 10.0.0.1 du routeur G1 comme passerelle par défaut. Le routeur G1 utilise l'adresse IP 10.0.0.2 du routeur G2 comme tronçon suivant lors du transfert du trafic vers le réseau de destination X.

Voici ce qui se produit lorsque l'hôte envoie un paquet au réseau de destination X :

1. La passerelle G1 avec l'adresse IP 10.0.0.1 reçoit un paquet de données de l'hôte 10.0.0.100 sur un réseau auquel elle est connectée.

2. La passerelle, G1, vérifie sa table de routage et obtient l'adresse IP 10.0.0.2 de la passerelle suivante, G2, sur la route vers le réseau de destination des paquets de données, X.

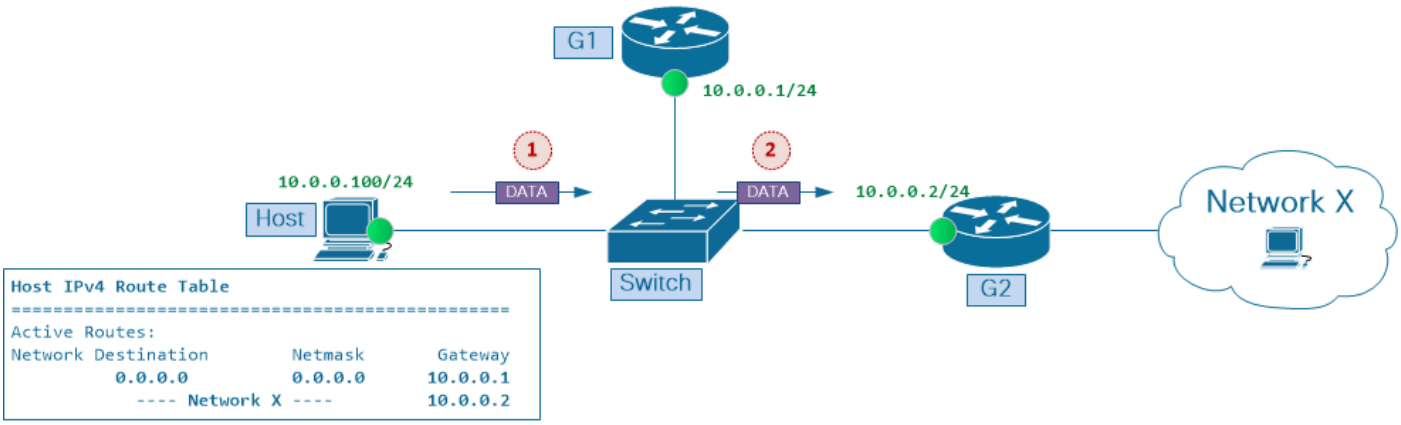
3. Si G2 et l'hôte identifié par l'adresse source du paquet IP se trouvent sur le même réseau, le message de redirection ICMP est envoyé à l'hôte. Le message de redirection ICMP conseille à l'hôte d'envoyer son trafic pour le réseau X directement à la passerelle G2, car il s'agit d'un chemin plus court vers la destination.

4. La passerelle G1 transmet le paquet de données d'origine à sa destination.

Selon la configuration de l'hôte, il peut choisir d'ignorer les messages de redirection ICMP que G1 lui envoie. Cependant, si l'hôte utilise les messages de redirection ICMP pour ajuster son cache de routage et commence à envoyer les paquets de données suivants directement à G2, ces avantages sont obtenus dans ce scénario

- Optimisation du chemin de transfert des données sur le réseau ; le trafic atteint sa destination plus rapidement.
- Réduction de l'utilisation des ressources réseau, telles que la bande passante et la charge CPU du routeur.

Image 2 - Saut suivant G2 installé dans le cache de routage de l'hôte



Saut suivant G2 installé dans le cache de routage d'hôte

Comme l'illustre l'image 2, une fois que l'hôte a créé une entrée de cache de route pour le réseau X avec G2 comme tronçon suivant, les avantages suivants sont visibles sur le réseau :

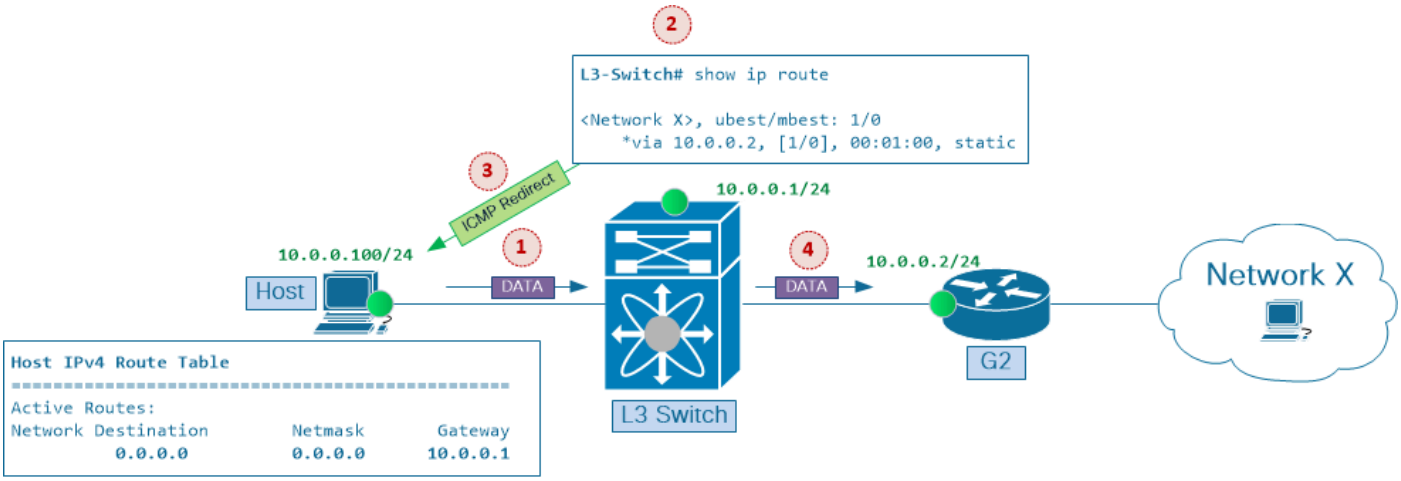
- L'utilisation de la bande passante sur la liaison entre le commutateur et le routeur G1 diminue dans les deux sens.
- L'utilisation du CPU sur le routeur G1 diminue parce que le flux de trafic de l'hôte vers le réseau X ne traverse plus ce noeud.
- Le délai réseau de bout en bout entre l'hôte et le réseau X s'améliore.

Pour comprendre l'importance du mécanisme de redirection ICMP, n'oubliez pas que les premières mises en oeuvre de routeur Internet reposaient principalement sur les ressources du processeur pour traiter le trafic de données. Par conséquent, il était souhaitable de réduire le volume de trafic qui devait être géré par un routeur unique et également de minimiser le nombre de sauts de routeur qu'un flux de trafic particulier devait traverser sur son chemin vers la destination. Dans le même temps, le transfert de couche 2 (également appelé commutation) a été principalement mis en oeuvre dans des circuits ASIC (Application-Specific Integrated Circuits) personnalisés et, du point de vue des performances de transfert, était relativement bon marché par rapport au transfert de couche 3 (également appelé routage), qui, là encore, a été effectué dans des processeurs à usage général.

Les générations ASIC plus récentes peuvent effectuer le transfert de paquets de couche 2 et de couche 3. La recherche dans la table de couche 3 effectuée dans le matériel permet de réduire les coûts de performances associés à la gestion des paquets par les routeurs. En outre, lorsque la fonctionnalité de transfert de couche 3 a été intégrée aux commutateurs de couche 2 (appelés désormais commutateurs de couche 3), elle a rendu le transfert de paquets plus efficace. Cela a éliminé le besoin d'options de conception de routeur à un bras (également appelé « router on a stick ») et évité les limitations associées à de telles configurations réseau.

L'image 3 repose sur le scénario de l'image 1. Désormais, les fonctions de couche 2 et de couche 3, fournies à l'origine par deux noeuds distincts, le commutateur et le routeur G1, sont consolidées dans un seul commutateur de couche 3, tel que la plate-forme Nexus 7000.

Image 3 - Le commutateur de couche 3 remplace la configuration à un routeur armé



Le commutateur de couche 3 remplace la configuration à un routeur armé

Voici ce qui se produit lorsque l'hôte envoie un paquet au réseau de destination X :

1. Le commutateur de passerelle L3 avec l'adresse IP 10.0.0.1 reçoit un paquet de données d'un hôte 10.0.0.100 sur un réseau auquel il est connecté.

2. La passerelle, le commutateur L3, vérifie sa table de routage et obtient l'adresse 10.0.0.2 de la passerelle suivante, G2, sur la route vers le réseau de destination des paquets de données, X.

3. Si G2 et l'hôte identifié par l'adresse source du paquet IP se trouvent sur le même réseau, le message de redirection ICMP est envoyé à l'hôte. Le message de redirection ICMP conseille à l'hôte d'envoyer son trafic pour le réseau X directement à la passerelle G2, car il s'agit d'un chemin plus court vers la destination.

4. La passerelle transmet le paquet de données d'origine à sa destination.

Les commutateurs de couche 3 étant désormais en mesure d'effectuer le transfert de paquets de couche 2 et de couche 3 au niveau ASIC, il est possible de conclure que les deux avantages de la fonctionnalité de redirection ICMP. Premièrement, l'amélioration du délai sur le réseau et, deuxièmement, la réduction de l'utilisation des ressources du réseau sont réalisées, et il n'est plus nécessaire d'accorder beaucoup d'attention aux techniques d'optimisation de chemin dans les segments Ethernet multipoints.

Cependant, avec la fonctionnalité de redirection ICMP activée sur les interfaces de couche 3, le transfert non optimal via des segments Ethernet multipoints continue de présenter des goulots d'étranglement potentiels, même si pour une raison différente, comme expliqué dans la section Considérations relatives à la plate-forme Nexus plus loin dans ce document.

Remarque : les redirections ICMP sont activées par défaut sur les interfaces de couche 3 dans les logiciels Cisco IOS® et Cisco NX-OS.

Remarque : résumé des conditions de génération des messages de redirection ICMP : le commutateur de couche 3 génère un message de redirection ICMP vers la source du paquet

---

de données, si le paquet de données doit être transféré vers l'interface de couche 3 sur laquelle ce paquet est reçu.

Chemins sous-optimaux via les réseaux Ethernet

Les protocoles IGP (Interior Gateway Protocol), tels que OSPF (Open Shortest Path First) et EIGRP (Cisco Enhanced Interior Gateway Routing Protocol), sont conçus pour synchroniser les informations de routage entre les routeurs et pour fournir un comportement de transfert de paquets cohérent et prévisible sur tous les noeuds de réseau qui respectent ces informations. Par exemple, avec les réseaux Ethernet multipoints, si tous les noeuds de couche 3 d'un segment utilisent les mêmes informations de routage et s'accordent sur le même point de sortie vers la destination, le transfert sous-optimal à travers ces réseaux est rarement le cas.

Pour comprendre les causes des chemins de transfert non optimaux, rappelez-vous que les noeuds de couche 3 prennent des décisions de transfert de paquets indépendantes les unes des autres. Autrement dit, la décision de transmission de paquets prise par le routeur B ne dépend pas de la décision de transmission de paquets prise par le routeur A. Il s'agit de l'un des principes clés à retenir lorsque vous dépannez le transfert de paquets via des réseaux IP. Il est important de le garder à l'esprit lorsque vous recherchez un chemin de transfert non optimal dans des réseaux Ethernet multipoints.

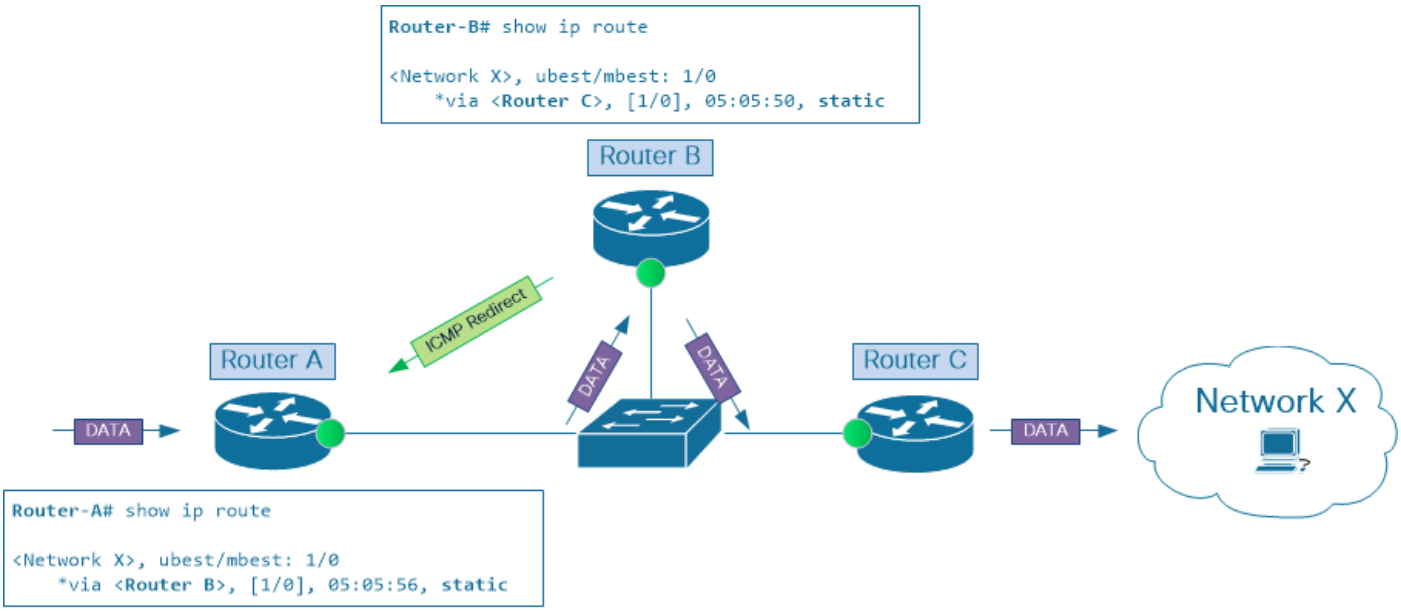
Comme mentionné précédemment, dans les réseaux où tous les routeurs s'appuient sur un protocole de routage dynamique unique pour acheminer le trafic entre les points d'extrémité, le transfert sous-optimal via des segments Ethernet multipoints ne doit pas se produire. Cependant, dans les réseaux réels, il est très courant de trouver une combinaison de divers mécanismes de routage et de transfert de paquets. Parmi ces mécanismes, citons les protocoles IGP, le routage statique et le routage basé sur des politiques. Ces fonctions sont généralement utilisées conjointement pour obtenir le transfert de trafic souhaité sur le réseau.

Bien que l'utilisation combinée de ces mécanismes puisse aider à affiner le flux de trafic et à répondre aux exigences d'une conception de réseau particulière, ils négligent les effets secondaires que ces outils peuvent provoquer dans les réseaux Ethernet multipoints et qui peuvent entraîner des performances réseau globales médiocres.

Routage statique

Pour illustrer cela, considérez le scénario de l'image 4. Le routeur A a une route statique vers le réseau X avec le routeur B comme tronçon suivant. En même temps, le routeur B utilise le routeur C comme tronçon suivant dans la route statique vers le réseau X.

Image 4 - Chemin non optimal avec routage statique



Chemin non optimal avec routage statique

Alors que le trafic entre dans ce réseau au niveau du routeur A, le quitte par le routeur C et finit par être acheminé vers le réseau de destination X, les paquets doivent traverser ce réseau IP deux fois avant d'atteindre la destination. Ceci n'est pas une utilisation efficace des ressources réseau. Au lieu de cela, envoyer des paquets du routeur A directement au routeur C permettrait d'obtenir les mêmes résultats, tout en consommant et en consommant moins de ressources réseau.

Remarque : même si dans ce scénario, les routeurs A et C sont utilisés comme noeuds de couche 3 d'entrée et de sortie pour ce segment de réseau IP, les deux noeuds peuvent être remplacés par des appliances de réseau (telles que des équilibreurs de charge ou des pare-feu) si ces derniers ont une configuration de routage qui entraîne le même comportement de transfert de paquets.

Policy-based routing

Le routage PBR (Policy Based Routing) est un autre mécanisme qui peut entraîner un chemin non optimal dans les réseaux Ethernet. Cependant, contrairement au routage statique ou dynamique, PBR ne fonctionne pas au niveau de la table de routage. Au lieu de cela, il programme la liste de contrôle d'accès (ACL) de redirection de trafic directement dans le matériel du commutateur. Par conséquent, pour certains flux de trafic, la recherche de transfert de paquets sur la carte de ligne d'entrée contourne les informations de routage obtenues via le routage statique ou dynamique.

Dans l'image 4, les routeurs A et B échangent des informations de routage sur le réseau de destination X avec l'un des protocoles de routage dynamique. Tous deux s'accordent à dire que le routeur B est le meilleur tronçon suivant vers ce réseau.

Cependant, avec une configuration PBR sur le routeur B qui remplace les informations de routage reçues du protocole de routage et définit le routeur C comme tronçon suivant vers le réseau X, la condition pour déclencher la fonction de redirection ICMP est remplie et le paquet est envoyé au

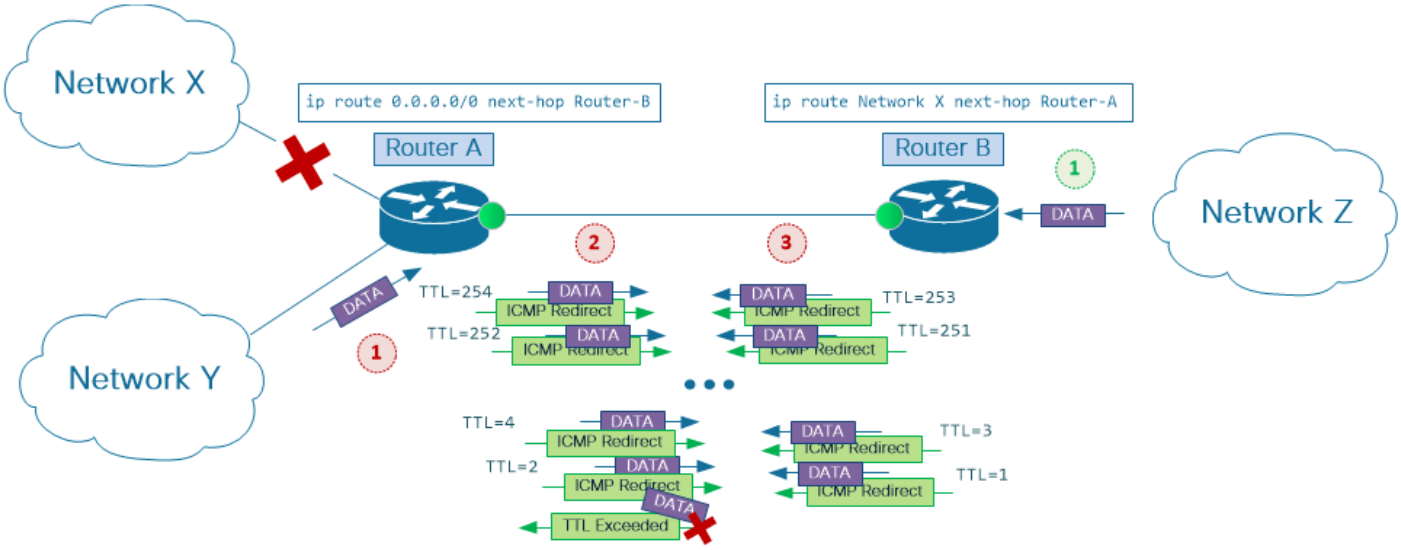
processeur du routeur B pour être traité plus avant.

Redirections ICMP sur des liaisons point à point

Jusqu'à présent, ce document faisait référence aux réseaux Ethernet auxquels sont connectés trois noeuds de couche 3 (ou plus), d'où le nom de réseaux Ethernet multipoints. Cependant, sachez que les messages de redirection ICMP peuvent également être générés sur des liaisons Ethernet point à point.

Considérez le scénario sur l'image 5. Le routeur A utilise la route statique par défaut pour envoyer le trafic au routeur B, tandis que le routeur B a une route statique vers le réseau X qui pointe vers le routeur A.

Image 5 - Redirections ICMP sur des liaisons point à point



Chemin non optimal avec routage statique

Cette option de conception, également connue sous le nom de connexion à résidence unique, est un choix populaire lorsque vous connectez des environnements de petits utilisateurs à des réseaux de fournisseurs de services. Ici, le routeur B est un périphérique Provider Edge (PE) et le routeur A est un périphérique User Edge (CE).

Notez que la configuration CE type inclut des routes statiques agrégées vers des blocs d'adresses IP utilisateur qui pointent vers l'interface Null0. Cette configuration est recommandée pour l'option de connectivité CE-PE à résidence unique avec routage statique. Toutefois, dans le cadre de cet exemple, supposons qu'aucune configuration de ce type n'est présente.

Supposez que le routeur A perd la connectivité au réseau X, comme illustré dans l'image. Lorsque des paquets provenant du réseau utilisateur Y ou du réseau distant Z tentent d'atteindre le réseau X, les routeurs A et B peuvent renvoyer le trafic entre eux et réduisent le champ de durée de vie IP dans chaque paquet jusqu'à ce que sa valeur atteigne 1, auquel point un routage supplémentaire du paquet n'est pas possible.

Alors que le trafic vers le réseau X rebondit entre les routeurs PE et CE, augmente considérablement (et inutilement) l'utilisation de la bande passante de la liaison CE-PE. Le problème s'aggrave si les redirections ICMP sont activées d'un côté ou des deux côtés de la connexion PE-CE point à point. Dans ce cas, chaque paquet du flux dirigé vers le réseau X est traité dans le processeur de chaque routeur plusieurs fois pour aider à générer les messages de redirection ICMP.

Considérations relatives à Nexus Platform

Lorsque les redirections ICMP sont activées sur l'interface de couche 3 et qu'un paquet de données entrant utilise cette interface pour entrer et sortir d'un commutateur de couche 3, un message de redirection ICMP est généré. Bien que le transfert de paquets de couche 3 soit effectué dans le matériel sur la plate-forme Cisco Nexus 7000, il incombe toujours au processeur du commutateur de construire des messages de redirection ICMP. Pour ce faire, le processeur du module de supervision Nexus 7000 doit obtenir des informations d'adresse IP du flux dont le chemin à travers le segment de réseau peut être optimisé. C'est la raison derrière le paquet de données envoyé par la carte de ligne d'entrée au module Supervisor.

Si les destinataires du message de redirection ICMP l'ignorent et continuent à transférer le trafic de données vers l'interface de couche 3 du commutateur Nexus sur lequel les redirections ICMP sont activées, le processus de génération de redirection ICMP est déclenché pour chaque paquet de données.

Au niveau de la carte de ligne, le processus commence sous la forme d'une exception de transfert matériel. Des exceptions sont soulevées sur les ASIC lorsque l'opération de transfert de paquets ne peut pas être effectuée avec succès par le module de carte de ligne. Dans ce cas, le paquet de données doit être envoyé au module Supervisor pour une gestion correcte des paquets.

Remarque : le CPU sur le module Supervisor ne génère pas seulement des messages de redirection ICMP, il gère beaucoup d'autres exceptions de transfert de paquets, telles que les paquets IP avec la valeur de durée de vie (TTL) définie sur 1, ou les paquets IP qui doivent être fragmentés avant d'être envoyés au saut suivant.

Une fois que le processeur du module Supervisor a envoyé le message de redirection ICMP à la source, il termine la gestion des exceptions en transférant le paquet de données au saut suivant via le module de carte de ligne de sortie.

Alors que les modules Supervisor Nexus 7000 utilisent des processeurs puissants capables de traiter de grands volumes de trafic, la plate-forme est conçue pour gérer la plupart du trafic de données au niveau de la carte de ligne sans qu'il soit nécessaire d'impliquer le processeur Supervisor CPU dans le processus de transfert de paquets. Cela permet au processeur de se concentrer sur ses tâches principales et laisse le transfert des paquets aux moteurs matériels dédiés sur les cartes de ligne.

Dans les réseaux stables, les exceptions de transfert de paquets, si elles se produisent, sont censées se produire à des taux raisonnablement faibles. Avec cette hypothèse, ils peuvent être

gérés par Supervisor CPU sans impact significatif sur ses performances. D'autre part, avec un processeur qui gère les exceptions de transfert de paquets qui se produisent à un taux très élevé peut avoir un effet négatif sur la stabilité et la réactivité globales du système.

La conception de la plate-forme Nexus 7000 fournit un certain nombre de mécanismes pour protéger le processeur du commutateur contre des quantités importantes de trafic. Ces mécanismes sont mis en oeuvre à différents points du système. Au niveau de la carte de ligne, il existe des limiteurs de débit matériels et un plan de contrôle Policing (CoPP). Les deux définissent des seuils de débit de trafic, qui contrôlent efficacement la quantité de trafic à transmettre au superviseur à partir de chaque module de carte de ligne.

Ces mécanismes de protection donnent la préférence au trafic de divers protocoles de contrôle qui sont critiques pour la stabilité du réseau et la facilité de gestion du commutateur, tels qu'OSPF, BGP ou SSH, et en même temps ils filtrent agressivement les types de trafic qui ne sont pas critiques pour la fonctionnalité du plan de contrôle du commutateur. La plupart du trafic de données, s'il est transféré au processeur à la suite d'exceptions de transfert de paquets, est fortement réglementé par de tels mécanismes.

Tandis que les limiteurs de débit matériel et CoPP policing les mécanismes assurent la stabilité du plan de contrôle du commutateur et sont fortement recommandés pour être toujours activés, ils peuvent être l'une des principales raisons des pertes de paquets de données, des retards de transfert et des performances applicatives globalement médiocres sur le réseau. C'est pourquoi il est important de comprendre les chemins empruntés par les flux de trafic sur le réseau et l'utilisation d'outils pour surveiller l'équipement réseau qui peut et/ou est censé utiliser la fonctionnalité de redirection ICMP.

Outils de surveillance et de diagnostic du trafic

show ip traffic

Les logiciels Cisco IOS et Cisco NX-OS permettent de vérifier les statistiques du trafic géré par le processeur. C'est fait avec **show ip traffic** erasecat4000_flash:. Cette commande peut être utilisée pour vérifier la réception et/ou la génération de messages de redirection ICMP par le commutateur ou le routeur de couche 3.

<#root>

Nexus7000#

show ip traffic | begin ICMP

```
ICMP Software Processed Traffic Statistics
--------------------------------------
Transmission:
Redirect: 1000, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

 ICMP originate Req: 0, Redirects Originate Req: 1000
 Originate deny - Resource fail: 0, short ip: 0, icmp: 0, others: 0
Reception:
 Redirect: 0, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

Nexus7000#
```

Exécutez la commande show ip traffic plusieurs fois et vérifiez si les compteurs de redirection ICMP s'incrémentent.

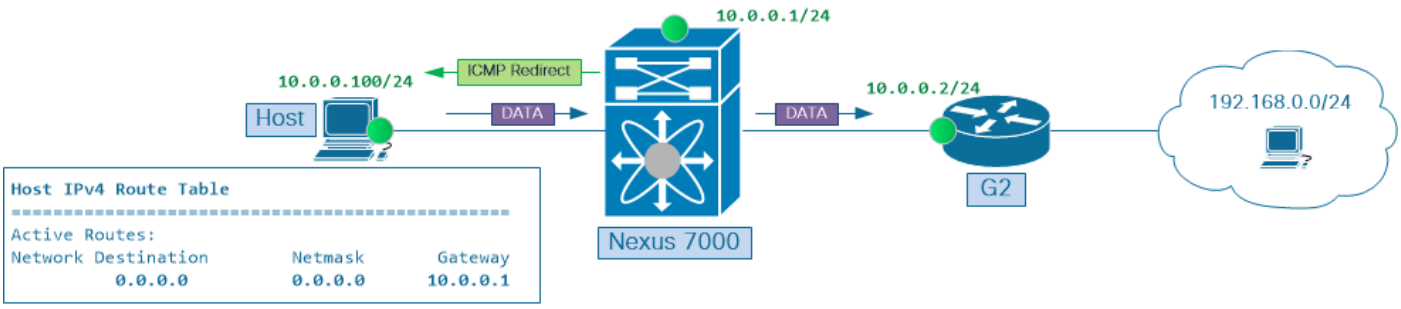
Ethanalyseur

Le logiciel Cisco NX-OS est doté d'un outil intégré pour capturer le trafic flowing vers et depuis le processeur du commutateur, connu sous le nom d'Ethanalyzer.

Remarque : pour plus d'informations sur Ethanalyzer, reportez-vous au Guide de dépannage d'Ethanalyzer on Nexus 7000.

L'image 6 présente un scénario similaire à celui de l'image 3. Ici, le réseau X est remplacé par le réseau 192.168.0.0/24.

Image 6 - Exécuter la capture Ethanalyzer



Exécuter la capture Ethanalyzer

L'hôte 10.0.0.100 envoie un flux continu de requêtes d'écho ICMP à l'adresse IP de destination 192.168.0.1. L'hôte utilise l'interface virtuelle de commutateur (SVI) 10 du commutateur Nexus 7000 comme tronçon suivant vers le réseau distant 192.168.0.0/24. À des fins de démonstration, l'hôte est configuré pour ignorer les messages de redirection ICMP.

Utilisez cette commande suivante pour capturer le trafic ICMP reçu et envoyé par le processeur

Nexus 7000 :

<#root>

```
Nexus7000#

ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000


Capturing on inband
2018-09-15 23:45:40.124077   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.124477     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.124533   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126344   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.126655   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request

    2018-09-15 23:45:40.128348   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128611     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
    2018-09-15 23:45:40.128659   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request

2018-09-15 23:45:40.130362   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130621     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.130669   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132392   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132652     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.132700   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134612     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.134660   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136598     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.136645   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138351   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.138656   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request

...
```

Les horodatages dans le résultat précédent suggèrent que trois paquets mis en évidence dans cet exemple ont été capturés en même temps, 2018-09-15 23:45:40.128. La suivante est une répartition par paquet de ce groupe de paquets

- Le premier paquet est le paquet de données d'entrée, qui dans cet exemple est une requête d'écho ICMP.

  2018-09-15 23:45:40.128348 10.0.0.100 -> 192.168.0.1 Requête d'écho ICMP (ping)

- Le deuxième paquet est un paquet de redirection ICMP, généré par la passerelle. Ce paquet est renvoyé à l'hôte.

  2018-09-15 23:45:40.128611 10.0.0.1 -> 10.0.0.100 Redirection ICMP (Redirection pour l'hôte)

- Le troisième paquet est le paquet de données capturé dans le sens de la sortie, après avoir

été routé par le processeur. Bien que cela ne soit pas illustré précédemment, la durée de vie IP de ce paquet est décrémentée et la somme de contrôle est recalculée.

2018-09-15 23:45:40.128659 10.0.0.100 -> 192.168.0.1 Requête d'écho ICMP (ping)

Lorsque vous parcourez de grandes captures Ethanalyzer qui contiennent de nombreux paquets de différents types et flux, il peut être difficile de corréler les messages de redirection ICMP avec le trafic de données qui leur correspond.

Dans ces situations, concentrez-vous sur les messages de redirection ICMP pour récupérer des informations sur les flux de trafic transférés de manière non optimale. Les messages de redirection ICMP incluent l'en-tête Internet plus les 64 premiers bits des données de datagramme d'origine. Ces données sont utilisées par la source du datagramme pour faire correspondre le message au processus approprié.

Utilisez l'outil de capture de paquets Ethanalyzer avec le mot clé detail pour afficher le contenu des messages ICMP Redirect et trouver les informations d'adresse IP du flux de données qui est transféré de manière sous-optimale.

<#root>

```
Nexus7000#

ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000 detail



...

Frame 2 (70 bytes on wire, 70 bytes captured)
 Arrival Time: Sep 15, 2018 23:54:04.388577000
 [Time delta from previous captured frame: 0.000426000 seconds]
 [Time delta from previous displayed frame: 0.000426000 seconds]
 [Time since reference or first frame: 0.000426000 seconds]
 Frame Number: 2
 Frame Length: 70 bytes
 Capture Length: 70 bytes
 [Frame is marked: False]
 [Protocols in frame: eth:ip:icmp:ip:icmp:data]
Ethernet II, Src: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf), Dst: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
 Destination: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
 Address: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
 .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
 .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
 Source: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
 Address: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
 .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
 .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
 Type: IP (0x0800)

Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.100 (10.0.0.100)


 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 0000 00.. = Differentiated Services Codepoint: Default (0x00)
```

```
 .... ..0. = ECN-Capable Transport (ECT): 0
 .... ...0 = ECN-CE: 0
 Total Length: 56
 Identification: 0xf986 (63878)
 Flags: 0x00
 0.. = Reserved bit: Not Set
 .0. = Don't fragment: Not Set
 ..0 = More fragments: Not Set
 Fragment offset: 0
 Time to live: 255
 Protocol: ICMP (0x01)
 Header checksum: 0xadd9 [correct]
 [Good: True]
 [Bad : False]
 Source: 10.0.0.1 (10.0.0.1)
 Destination: 10.0.0.100 (10.0.0.100)
```

Internet Control Message Protocol

Type: 5 (Redirect)

Code: 1 (Redirect for host)

```
 Checksum: 0xb8e5 [correct]
 Gateway address: 10.0.0.2 (10.0.0.2)
 Internet Protocol, Src: 10.0.0.100 (10.0.0.100), Dst: 192.168.0.1 (192.168.0.1)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 0000 00.. = Differentiated Services Codepoint: Default (0x00)
 .... ..0. = ECN-Capable Transport (ECT): 0
 .... ...0 = ECN-CE: 0
 Total Length: 84
 Identification: 0xf986 (63878)
 Flags: 0x00
 0.. = Reserved bit: Not Set
 .0. = Don't fragment: Not Set
 ..0 = More fragments: Not Set
 Fragment offset: 0
 Time to live: 254
 Protocol: ICMP (0x01)
 Header checksum: 0xa8ae [correct]
 [Good: True]
 [Bad : False]
 Source: 10.0.0.100 (10.0.0.100)
 Destination: 192.168.0.1 (192.168.0.1)
 Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0 ()
 Checksum: 0x02f9 [incorrect, should be 0xcae1]
Identifier: 0xa01d
Sequence number: 36096 (0x8d00)

...
```

Désactiver les redirections ICMP

Si la conception du réseau exige que le flux de trafic soit acheminé à partir de la même interface de couche 3 sur laquelle il est entré dans le commutateur ou le routeur, il est possible d'empêcher le flux d'être acheminé via le processeur si vous désactivez la fonctionnalité de redirection ICMP sur l'interface de couche 3 qui lui correspond.

En fait, pour la plupart des réseaux, il est conseillé de désactiver de manière proactive les redirections ICMP sur toutes les interfaces de couche 3, à la fois physiques, comme les interfaces Ethernet, et virtuelles, comme les interfaces Port-Channel et SVI. Utilisez no ip redirects Commande de niveau interface de Cisco NX-OS pour désactiver les redirections ICMP sur une interface de couche 3. Pour vérifier que la fonctionnalité de redirection ICMP est désactivée :

- Garantir**no ip** redirects est ajoutée à la configuration d'interface.

<#root>

```
Nexus7000#
show run interface vlan 10


interface Vlan10
  no shutdown


no ip redirects
  ip address 10.0.0.1/24
```

- Assurez-vous que l'état des redirections ICMP sur l'interface indique disabled.

<#root>

```
Nexus7000#
show ip interface vlan 10 | include redirects
  IP icmp redirects:
disabled
```

- Assurez-vous que l'indicateur d'activation/désactivation de redirection ICMP est défini sur 0 par le composant logiciel Cisco NX-OS qui pousse la configuration d'interface du commutateur Supervisor vers une ou plusieurs cartes de ligne.

<#root>

```
Nexus7000#
show system internal eltm info interface vlan 10 | i icmp_redirect
  per_pkt_ls_en = 0,
icmp_redirect = 0
, v4_same_if_check = 0
```

- Assurez-vous que l'indicateur d'activation/désactivation de la redirection ICMP pour une interface de couche 3 particulière est défini sur 0 sur une ou plusieurs cartes de ligne.

<#root>

```
Nexus7000#
attach module 7


Attaching to module 7 ...
To exit type 'exit', to abort type '$.'
Last login: Wed Sep 15 23:56:25 UTC 2018 from 127.1.1.1 on pts/0
module-7#

!--- Optionally, jump to non-admin Virtual Device Context (VDC) if verification needs to be done in one
module-7#
vdc 6



module-7#
show system internal iftmc info interface vlan 10 | include icmp_redirect



icmp_redirect : 0x0
 ipv6_redirect : 0x1
```

Résumé

Le mécanisme de redirection ICMP, tel que décrit dans la RFC 792, a été conçu pour optimiser le chemin de transfert via des segments de réseau multipoint. Au début d'Internet, cette optimisation a permis de protéger des ressources réseau coûteuses, telles que la bande passante de liaison et les cycles CPU des routeurs. À mesure que la bande passante du réseau devenait plus abordable et que le routage de paquets basé sur le processeur, relativement lent, évoluait vers un transfert de paquets de couche 3 plus rapide dans les circuits ASIC matériels dédiés, l'importance du transit optimal des données via les segments de réseau multipoint diminuait. Par défaut, la

fonctionnalité de redirection ICMP est activée sur chaque interface de couche 3. Cependant, ses tentatives d’informer les noeuds réseau sur des segments Ethernet multipoints des chemins de transfert optimaux ne sont pas toujours comprises et prises en compte par le personnel du réseau. Dans les réseaux utilisant conjointement divers mécanismes de transfert, tels que le routage statique, le routage dynamique et le routage basé sur des politiques, si vous laissez la fonctionnalité de redirection ICMP activée et que vous ne la surveillez pas correctement, cela peut entraîner une utilisation indésirable du processeur du ou des noeuds de transit pour gérer le trafic de production. Cela peut à son tour avoir un impact significatif sur les flux de trafic de production et sur la stabilité du plan de contrôle de l'infrastructure réseau.

Pour la plupart des réseaux, il est recommandé de désactiver de manière proactive la fonctionnalité de redirection ICMP sur toutes les interfaces de couche 3 de l'infrastructure réseau. Cela permet d'éviter les scénarios de trafic de données de production qui est géré dans le processeur des commutateurs et routeurs de couche 3 lorsqu'il y a un meilleur chemin de transfert à travers des segments de réseau multipoints.

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.