Options de qualité de service sur les interfaces de tunnel GRE

Contenu

Introduction

Ce document passe en revue les fonctionnalités QoS (Quality of Service) qui peuvent être configurées sur des interfaces de tunnel à l'aide de l'encapsulation de routage générique (GRE). Les tunnels configurés avec la sécurité IP (IPSec) sont hors de portée de ce document.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Présentation de GRE

Avant d'en savoir plus sur la QoS sur les tunnels GRE, vous devez d'abord comprendre le format d'un paquet tunnelisé.

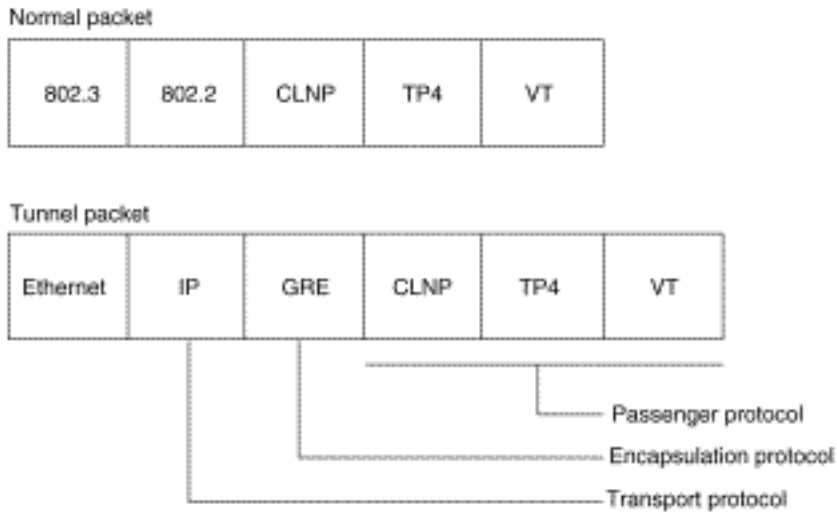
Une interface de tunnel est une interface virtuelle ou logique sur un routeur exécutant le logiciel Cisco IOS®. Il crée une liaison point à point virtuelle entre deux routeurs Cisco situés à des points distants sur un interréseau IP.

GRE est un protocole d'encapsulation pris en charge par IOS et défini dans RFC 1702 . Les protocoles de tunnellisation encapsulent les paquets à l'intérieur d'un protocole de transport.

Une interface de tunnel prend en charge un en-tête pour chacun de ces éléments :

- Protocole passager ou protocole encapsulé, tel que IP, AppleTalk, DECnet ou IPX.
- Un protocole porteur (GRE dans ce cas).
- Protocole de transport (IP uniquement dans ce cas).

Le format d'un paquet de tunnel est illustré ici :



Référez-vous à Configuration des interfaces logiques pour plus d'informations sur la configuration des tunnels GRE.

QoS Cisco pour tunnels GRE

Une interface de tunnel prend en charge plusieurs des mêmes fonctions QoS qu'une interface physique. Ces sections décrivent les fonctions QoS prises en charge.

Mise en forme

Le logiciel Cisco IOS version 12.0(7)T a introduit la prise en charge de l'application du formatage de trafic générique (GTS) directement sur l'interface de tunnel. L'exemple de configuration suivant forme l'interface de tunnel à un débit de sortie global de 500 kbits/s. Référez-vous à Configuration du formatage du trafic générique pour plus d'informations.

```
interface Tunnel0
  ip address 130.1.2.1 255.255.255.0
  traffic-shape rate 500000 125000 125000 1000
  tunnel source 10.1.1.1
  tunnel destination 10.2.2.2
```

Le logiciel Cisco IOS Version 12.1(2)T a ajouté la prise en charge du formatage basé sur les classes à l'aide de l'interface de ligne de commande (MQC) QoS modulaire. L'exemple de configuration suivant montre comment appliquer la même politique de mise en forme à l'interface de tunnel avec les commandes MQC. Référez-vous à Configuration du formatage basé sur les classes pour plus d'informations.

```
policy-map tunnel
  class class-default
    shape average 500000 125000 125000
interface Tunnel0
  ip address 130.1.2.1 255.255.255.0
  service-policy output tunnel
  tunnel source 130.1.35.1
  tunnel destination 130.1.35.2
```

Contrôle

Lorsqu'une interface devient encombrée et que les paquets commencent à mettre en file d'attente, vous pouvez appliquer une méthode de mise en file d'attente aux paquets en attente de transmission. Les interfaces logiques Cisco IOS ne prennent pas en charge un état d'encombrement et ne prennent pas en charge l'application directe d'une stratégie de service qui applique une méthode de mise en file d'attente. Au lieu de cela, vous devez appliquer une stratégie hiérarchique comme suit :

1. Créez une stratégie de niveau enfant ou inférieur qui configure un mécanisme de mise en file d'attente, comme la mise en file d'attente à faible latence avec la commande **priority** et la mise en file d'attente pondérée basée sur les classes (CBWFQ) avec la commande **bandwidth**. Référez-vous à Gestion des encombrements pour plus d'informations.
   ```
   policy-map child
    class voice
     priority 512
   ```
2. Créez une stratégie de niveau supérieur ou parent qui applique le formatage basé sur les classes. Appliquez la stratégie enfant en tant que commande sous la stratégie parent puisque le contrôle d'admission pour la classe enfant est effectué en fonction du taux de mise en forme de la classe parent.
   ```
   policy-map tunnel
    class class-default
     shape average 2000000
     service-policy child
   ```
3. Appliquez la stratégie parent à l'interface de tunnel.
   ```
   interface tunnel0
      service-policy tunnel
   ```

Le routeur imprime ce message de journal lorsqu'une interface de tunnel est configurée avec une stratégie de service qui applique la mise en file d'attente sans mise en forme.

```
router(config)# interface tunnel1
router(config-if)# service-policy output child
 Class Based Weighted Fair Queueing not supported on this interface
```

Les interfaces de tunnel prennent également en charge la réglementation basée sur les classes, mais elles ne prennent pas en charge le débit d'accès garanti (CAR).

Remarque : les stratégies de service ne sont pas prises en charge sur les interfaces de tunnel sur 7500.

Évitement de la congestion

La version 11.3T du logiciel Cisco IOS a introduit le marquage de tunnel GRE et les valeurs de priorité DSCP ou IP, qui configurent le routeur pour copier les valeurs de bit de priorité IP de l'octet ToS dans le tunnel ou l'en-tête IP GRE qui encapsule le paquet interne. Auparavant, ces bits étaient définis sur zéro. Les routeurs intermédiaires entre les points d'extrémité du tunnel peuvent utiliser les valeurs de priorité IP pour classer les paquets pour les fonctionnalités QoS telles que le routage de stratégie, WFQ et la détection précoce aléatoire pondérée (WRED).

La commande qos pre-classify

Lorsque les paquets sont encapsulés par des en-têtes de tunnel ou de chiffrement, les fonctions QoS ne peuvent pas examiner les en-têtes de paquet d'origine et classer correctement les paquets. Les paquets traversant le même tunnel ont les mêmes en-têtes de tunnel, de sorte que les paquets sont traités de manière identique si l'interface physique est congestionnée. Avec l'introduction de la fonctionnalité Qualité de service pour les réseaux privés virtuels (VPN), les paquets peuvent désormais être classés avant la transmission tunnel et le chiffrement.

Dans cet exemple, tunnel0 est le nom du tunnel. La commande **qos pre-classify** active la fonctionnalité QoS pour VPN sur le tunnel0 :

```
Router(config)# interface tunnel0
Router(config-if)# qos pre-classify
```

Remarque : La commande **qos pre-classify** peut être utilisée afin de classer le trafic en fonction de valeurs autres que la priorité IP ou DSCP. Par exemple, vous pouvez classer les paquets en fonction du flux IP ou des informations de couche 3, telles que l'adresse IP source et de destination pour laquelle cette commande peut être utilisée. La commande **qos pre-classify** n'est requise que si vous classifiez le trafic sur IP, protocole ou port. Si la classification est basée sur le code DSCP, la **préclassification qos** n'est pas requise.

Caractérisation du trafic pour les politiques QoS

Lors de la configuration d'une stratégie de service, vous devrez peut-être d'abord caractériser le trafic qui traverse le tunnel. Cisco IOS prend en charge la comptabilité Netflow et IP Cisco Express Forwarding (CEF) sur les interfaces logiques telles que les tunnels. Reportez-vous au Guide des solutions de services NetFlow pour plus d'informations.

Où appliquer la stratégie de service ?

Vous pouvez appliquer une stratégie de service à l'interface de tunnel ou à l'interface physique sous-jacente. La décision d'appliquer la politique dépend des objectifs de QoS. Cela dépend également de l'en-tête que vous devez utiliser pour la classification.

- Appliquez la stratégie à l'interface de tunnel sans **qos-preclassify** lorsque vous voulez classifier les paquets en fonction de l'en-tête de pré-tunnel.
- Appliquez la stratégie à l'interface *physique* sans **qos-preclassify** lorsque vous voulez classifier les paquets en fonction de l'en-tête post-tunnel. En outre, appliquez la stratégie à l'interface physique lorsque vous voulez formater ou contrôler tout le trafic appartenant à un tunnel, et l'interface physique prend en charge plusieurs tunnels.
- Appliquez la stratégie à une interface *physique* et activez **qos-preclassify** sur une interface de tunnel lorsque vous voulez classifier les paquets en fonction de l'en-tête de pré-tunnel.

Interfaces de tunnel multipoint

Le formatage CBWFQ interne basé sur les classes n'est pas pris en charge sur une interface multipoint. L'ID de bogue Cisco CSCds87191 configure le routeur pour imprimer un message d'erreur lors du rejet de la stratégie.

Problèmes identifiés

Dans de rares conditions, l'application d'une stratégie de service configurée avec la commande **shape** entraîne des erreurs d'utilisation et d'alignement élevés du processeur. La charge CPU est causée par la consignation des erreurs d'alignement, qui sont à leur tour causées par CEF qui définit incorrectement l'interface de sortie et les informations de réécriture de contiguïté. Ce problème n'affecte que les plates-formes non RSP (de bas de gamme) et les plates-formes utilisant la commutation CEF basée sur les particules, et est résolu via les ID de bogue Cisco CSCdu45504 et CSCuk30302. Vous pouvez également envisager les solutions suivantes :

- Remplacez l'encapsulation GRE par **ipip en mode tunnel**.
- Remplacez la commande **shape** par la commande **police**.
- Configurez le formatage sur l'interface physique prenant en charge le tunnel.

Informations connexes

- Qualité de service pour les réseaux privés virtuels
- Configuration d'un tunnel GRE sur câble
- Assistance technique sur la technologie QoS
- Configuration d'un tunnel GRE sur IPSec avec OSPF
- Support et documentation techniques - Cisco Systems