Options de qualité de service sur les interfaces de tunnel GRE

Contenu

Introduction

Ce document passe en revue que des caractéristiques de Qualité de service (QoS) peuvent être configuré sur des interfaces de tunnel utilisant 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.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Aperçu de GRE

Avant d'apprendre au sujet de QoS au-dessus de GRE perce un tunnel, vous le premier besoin de comprendre le format d'un paquet percé un tunnel.

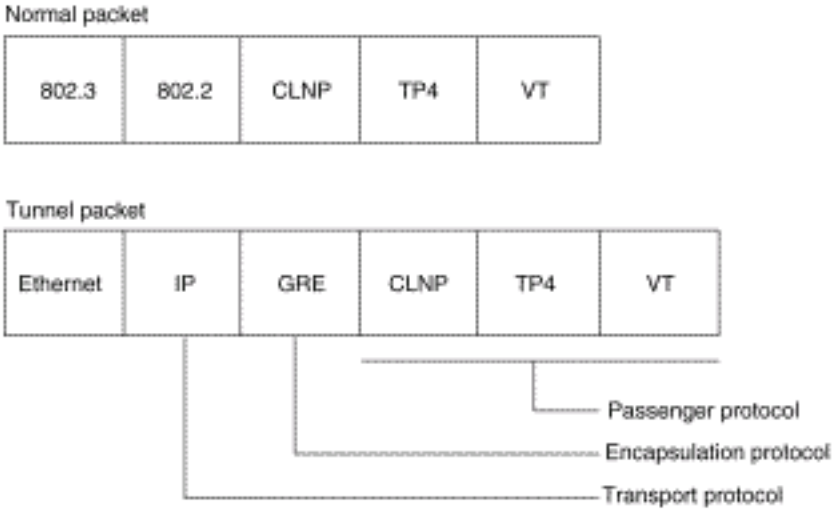
Une interface de tunnel est une virtuelle ou une interface logique sur un logiciel courant de Cisco IOS® de routeur. Il crée un lien point par point virtuel entre deux Routeurs de Cisco aux points distants au-dessus d'une interconnexion de réseaux IP.

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

Une interface de tunnel prend en charge une en-tête pour chacune de ces derniers :

- Un protocole passager ou un protocole encapsulé, tel que l'IP, l'AppleTalk, le DECNet, ou l'IPX.
- Un protocole transporteur (GRE dans ce cas).
- Un protocole de transport (IP seulement dans ce cas).

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



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

Cisco QoS pour des tunnels GRE

Une interface de tunnel prend en charge plusieurs des mêmes caractéristiques de QoS comme

interface physique. Ces sections décrivent les caractéristiques prises en charge de QoS.

Formation

Le logiciel Release12.0(7)T de Cisco IOS a introduit le soutien d'appliquer le Formatage du trafic générique (GTS) directement sur l'interface de tunnel. La configuration d'échantillon suivante forme l'interface de tunnel à un débit sortant global de 500 Kbps. Référez-vous à configurer le pour en savoir plus de Formatage du trafic générique.

```
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 le soutien de la formation basée sur classe utilisant l'interface de ligne de commande modulaire de QoS (MQC). La configuration d'échantillon suivante affiche comment s'appliquer la même stratégie de mise en forme à l'interface de tunnel avec les commandes MQC. Référez-vous à configurer le pour en savoir plus de formation basé sur classe.

```
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
```

Maintien de l'ordre

Quand une interface devient début congestionné et de paquets pour s'aligner, vous pouvez s'appliquer une méthode de mise en file d'attente aux paquets attendant d'être transmis. Les interfaces logiques de Cisco IOS en soi ne prennent en charge pas un état d'encombrement et ne prennent en charge pas 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 politique hiérarchique comme suit :

1. Créez un « enfant » ou la stratégie de plus bas niveau qui configurent un mécanisme de mise en file d'attente, tel que la basse latence s'alignant avec la commande et le Mise en file d'attente pondérée basée sur les classes (CBWFQ) **prioritaire** avec la **commande bandwidth**. Référez-vous au pour en savoir plus de Gestion d'encombrement.`policy-map child`
   ```
   class voice
    priority 512
   ```
2. Créez un « parent » ou la stratégie de niveau supérieur qui appliquent la formation basée sur classe. Appliquez la stratégie enfant comme commande dans le cadre de la stratégie de parent puisque le contrôle d'admission pour la classe enfant est fait a basé sur le taux de mise en forme pour la classe parente.`policy-map tunnel`
   ```
   class class-default
    shape average 2000000
    service-policy child
   ```
3. Appliquez-vous la stratégie de parent à l'interface de tunnel.`interface tunnel0`
   ```
    service-policy tunnel
   ```

Le routeur imprime ce message de log quand une interface de tunnel est configurée avec une stratégie de service qui applique la Mise en file d'attente sans formation.

```
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 en charge également le maintien de l'ordre basé sur classe, mais elles ne prennent en charge pas le Fonction Committed Access Rate (CAR).

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

Manière d'éviter d'encombrement

La version du logiciel Cisco IOS 11.3T a introduit le marquage de tunnel GRE et le DSCP ou les valeurs de Priorité IP, qui configure le routeur copier les valeurs de bit de priorité IP de l'octet de tos sur le tunnel ou l'en-tête IP GRE qui encapsule le paquet interne. Précédemment, ces bits ont été placés à zéro. Les routeurs intermédiaires entre les périphériques du tunnel peuvent employer les valeurs de Priorité IP pour classifier les paquets pour des caractéristiques de QoS telles que le routage de stratégie, le WFQ, et le Détection précoce directe pondérée (WRED).

La commande de qos pre-classify

Quand des paquets sont encapsulés par des en-têtes de tunnel ou de cryptage, les caractéristiques de QoS ne peuvent pas examiner les en-têtes du paquet d'origine et classifier correctement les paquets. Les paquets voyageant à travers le même tunnel ont les mêmes en-têtes de tunnel, ainsi les paquets sont traités identiquement si l'interface physique est congestionnée. Avec l'introduction de la qualité de service pour la caractéristique de Réseaux privés virtuels (VPN), des paquets peuvent maintenant être classifiés avant que le perçage d'un tunnel et le cryptage se produisent.

Dans cet exemple, tunnel0 est le nom de tunnel. Les commandes enables de **qos pre-classify que le** QoS pour VPN comporte sur tunnel0 :

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

Remarque: La commande de **qos pre-classify** peut être utilisée afin de classifier le trafic basé sur des valeurs autres que la Priorité IP ou le DSCP. Par exemple, vous pourriez vouloir classifier des paquets basés sur l'ip flow ou poser les informations 3, telles que la source et l'adresse IP de destination pour lesquelles cette commande peut être utilisée. La commande de **qos pre-classify** est exigée seulement si vous classifiez le trafic sur l'IP, le protocole, ou le port. Si la classification est basée sur le code de DSCP, alors le **qos pre-classify** n'est pas exigé.

Spécification du trafic pour des stratégies QoS

En configurant une stratégie de service, vous pourriez devoir la première fois caractériser le trafic qui traverse le tunnel. Le Cisco IOS prend en charge le NetFlow et le Technologie Cisco Express Forwarding (CEF) IP rendant compte sur des interfaces logiques comme des tunnels. Référez-vous au pour en savoir plus de guide de solutions de services Netflow.

D'où applique-t-je la stratégie de service ?

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

- Appliquez-vous la stratégie à l'interface de tunnel sans **qos-preclassify** quand vous voulez classifier des paquets basés sur l'en-tête de pré-tunnel.
- Appliquez-vous la stratégie à l'*interface physique* sans **qos-preclassify** quand vous voulez classifier des paquets basés sur l'en-tête de POST-tunnel. En outre, appliquez-vous la stratégie à l'interface physique quand vous voulez former ou maintenir l'ordre tout le trafic appartenant à un tunnel, et l'interface physique prend en charge plusieurs tunnels.
- Appliquez-vous la stratégie à une *interface physique* et l'enable **qos-preclassify** sur une interface de tunnel quand vous voulez classifier des paquets basés sur l'en-tête de pré-tunnel.

Interfaces de tunnel multipoints

CBWFQ à l'intérieur de la formation basée sur classe 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 en rejetant la stratégie.

Problèmes identifiés

Dans les rares conditions, l'application d'une service-stratégie configurée avec la commande de **forme** mène aux erreurs d'utilisation du CPU élevé et de cadrage. Le chargement CPU est provoqué par en se connectant les erreurs de cadrage, qui sont provoqué par à leur tour par le CEF plaçant inexactement les informations d'interface de sortie et de réécriture de contiguïté. Ce problème affecte seulement des Plateformes de non-RSP (bas) et des Plateformes utilisant la commutation basée sur particule de CEF, et est résolu par l'intermédiaire des id CSCdu45504 et CSCuk30302 de bogue Cisco. Vous pouvez également considérer ces contournements :

- Remplacez l'encapsulation GRE par l'**ipip de tunnel mode**.
- Remplacez la commande de **forme** par l'ordre de **police**.
- Configure formant sur l'interface physique prenant en charge le tunnel.

Informations connexes

- Qualité de service pour des 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