Présentation des compteurs de paquets dans la sortie de la commande show interface rate avec CAR (Committed Access Rate)

Contenu

Introduction

Le Committed Access Rate (CAR) est une fonctionnalité de limitation du débit pouvant servir à offrir des services de classification et de contrôle. Le CAR peut être utilisé pour classer des paquets selon certains critères tels que l'adresse IP et les valeurs de port qui utilisent des listes d'accès. Les mesures à prendre peuvent être définies pour les paquets qui respectent la valeur limite de débit et pour ceux qui la dépassent. Consultez le document Configurer le Committed Access Rate pour en savoir plus sur la configuration du CAR.

Ce document explique pourquoi la sortie de la commande **show interface x/x rate-limit** montre une valeur `non nulle en bits/s dépassée` lorsque la valeur `conforme en bits/s` est inférieure au débit d'informations garanti configuré (CIR).

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Conventions relatives aux conseils techniques Cisco.

Présentation du résultat de la commande show interface rate

Il existe trois conditions dans lesquelles vous pouvez voir des débits supérieurs non nuls dans la sortie de cette commande :

- Les valeurs de rafales sont trop basses pour permettre un débit suffisant. Par exemple, consultez l'ID de bogue Cisco CSCdw42923 (clients enregistrés uniquement).
- Problème résolu avec double comptabilisation dans le logiciel Cisco IOS®
- bogue logiciel dans Cisco IOS

Regardez l'exemple de sortie d'une interface d'accès virtuel. Dans cette configuration, RADIUS est utilisé afin d'attribuer une limite de débit à l'interface d'accès virtuel créée dynamiquement.

```
AV Pair from Radius
Cisco-AVPair = "lcp:interface-config#1=rate-limit input 256000 7500 7500
conform-action continue
exceed-action drop",
Cisco-AVPair = "lcp:interface-config#2=rate-limit output 512000 7500 7500
conform-action continue
exceed-action drop",
```

Utilisez la commande show interface x rate-limit afin de surveiller les performances du contrôleur Cisco existant, CAR. Dans cet exemple, le résultat de cette commande fournit des indications sur la raison pour laquelle il y a un débit supérieur à zéro. La valeur de rafale actuelle est de 7 392 octets, tandis que la valeur de rafale validée (Bc), indiquée par la valeur limite, est définie sur 7 500 octets.

```
router#show interfaces virtual-access 26 rate-limit
Virtual-Access26 Cable Customers
  Input
    matches: all traffic
      params:  256000 bps, 7500 limit, 7500 extended limit
      conformed 2248 packets, 257557 bytes; action: continue
      exceeded 35 packets, 22392 bytes; action: drop
      last packet: 156ms ago, current burst: 0 bytes
      last cleared 00:02:49 ago, conformed 12000 bps, exceeded 1000 bps
  Output
    matches: all traffic
      params:  512000 bps, 7500 limit, 7500 extended limit
      conformed 3338 packets, 4115194 bytes; action: continue
      exceeded 565 packets, 797648 bytes; action: drop
      last packet: 188ms ago, current burst: 7392 bytes
      last cleared 00:02:49 ago, conformed 194000 bps, exceeded 37000 bps
```

Lorsque vous configurez CAR ou un régulateur plus récent de Cisco, la réglementation basée sur les classes, vous devez configurer des valeurs de rafales suffisamment élevées pour garantir le débit attendu et pour vous assurer que le régulateur abandonne les paquets uniquement pour punir la congestion à court terme.

Lorsque vous sélectionnez des valeurs de rafale, il est important de prendre en charge les augmentations transitoires de la taille de la file d'attente. Vous ne pouvez pas simplement supposer que les paquets arrivent et partent en même temps. Vous ne pouvez pas non plus présumer que la file d'attente passe de vide à un paquet et que la file d'attente reste à un paquet

en fonction d'une heure d'arrivée d'entrée/sortie cohérente. Si le trafic type est assez dense, les valeurs de rafales doivent être proportionnellement importantes pour permettre le maintien de l'utilisation de la liaison à un niveau acceptable. Une taille de rafale trop faible ou un seuil minimal trop faible peut entraîner une utilisation de liaison inacceptable.

Une rafale peut être définie simplement comme une série de trames de taille MTU dos à dos, telles que des trames de 1 500 octets qui proviennent d'un réseau Ethernet. Lorsqu'une rafale de trames arrive à une interface de sortie, elle peut submerger les tampons de sortie et dépasser la profondeur configurée du seau de jeton à un moment instantané dans le temps. Avec l'utilisation d'un système de contrôle de jeton, un régulateur prend une décision binaire pour déterminer si un paquet entrant est conforme, dépasse ou viole les valeurs de contrôle configurées. Avec le trafic en rafale, tel qu'un flux FTP, le taux d'arrivée instantané de ces paquets peut dépasser les valeurs de rafales configurées et conduire à des abandons CAR.

En outre, le débit global en période de congestion varie en fonction du type de trafic évalué par le régulateur. Bien que le trafic TCP soit sensible à la congestion, les autres flux ne le sont pas. Les paquets basés sur UDP et ICMP sont des exemples de flux non réactifs.

TCP est basé sur un accusé de réception positif avec retransmission. TCP utilise une fenêtre glissante dans le cadre de son mécanisme d'accusé de réception positif. Les protocoles de fenêtre glissante utilisent mieux la bande passante du réseau car ils permettent à l'expéditeur de transmettre plusieurs paquets avant d'attendre un accusé de réception. Par exemple, dans un protocole de fenêtre glissante avec une taille de fenêtre de 8, l'expéditeur est autorisé à transmettre 8 paquets avant de recevoir un accusé de réception. Si vous augmentez la taille de la fenêtre, le temps d'inactivité du réseau est largement éliminé. Un protocole de fenêtre glissante bien ajusté maintient le réseau complètement saturé par les paquets et maintient un débit élevé.

Puisque les points d'extrémité ne connaissent pas l'état d'encombrement spécifique du réseau, le protocole TCP en tant que protocole est conçu pour réagir à l'encombrement du réseau en réduisant ses débits de transmission en cas d'encombrement. Plus précisément, il utilise deux techniques :

Technique	Description
Réduction multiplicative de la congestion	En cas de perte d'un segment (équivalent d'un paquet au protocole TCP), réduisez de moitié la fenêtre d'encombrement. La fenêtre d'encombrement est une deuxième valeur ou fenêtre qui est utilisée pour limiter le nombre de paquets qu'un expéditeur peut transmettre sur le réseau avant d'attendre un accusé de réception.
Récupération de démarrage lente	Lorsque vous démarrez le trafic sur une nouvelle connexion ou augmentez le trafic après une période d'encombrement, démarrez la fenêtre d'encombrement à la taille d'un seul segment et augmentez la fenêtre d'encombrement d'un segment chaque fois qu'un accusé de réception arrive. TCP initialise la fenêtre d'encombrement sur 1, envoie un segment initial et attend. Lorsque l'accusé de réception arrive, il augmente la fenêtre d'encombrement à 2, envoie deux segments et attend. Pour plus de détails, voir

	RFC 2001 .

Les paquets peuvent être perdus ou détruits lorsque des erreurs de transmission interfèrent avec les données, lorsque le matériel réseau tombe en panne ou lorsque les réseaux deviennent trop chargés pour prendre en charge la charge présentée. Le protocole TCP suppose que les paquets perdus, ou les paquets qui ne sont pas reconnus dans l'intervalle de temps en raison d'un délai extrême, indiquent une congestion du réseau.

Le système de contrôle de groupement de jetons d'un régulateur est appelé à chaque arrivée de paquet. Plus précisément, le taux conforme et le taux supérieur sont calculés à partir de cette formule simple :

```
(conformed bits since last clear counter)/(time in seconds elapsed since last clear counter)
```

Puisque la formule calcule les taux sur une période à partir de la dernière fois que les compteurs ont été effacés, Cisco recommande d'effacer les compteurs afin de surveiller le taux actuel. Si les compteurs ne sont pas effacés, le taux de formule précédent signifie que la sortie de la commande **show** affiche une moyenne calculée sur une période potentiellement très longue et que les valeurs ne sont peut-être pas significatives dans la détermination du taux actuel.

Le débit moyen doit correspondre au débit de données garanti (CIR) configuré sur une période donnée. Les tailles de rafales permettent une durée de rafale maximale à un moment donné. S'il n'y a pas de trafic ou moins que la valeur du CIR du trafic et que le compartiment de jeton ne se remplit pas, une très grande rafale reste limitée à une taille particulière calculée en fonction de la rafale normale et de la rafale étendue.

Le taux de chute résulte de ce mécanisme

1. Notez l'heure actuelle.
2. Mettez à jour le saut de jeton avec le nombre de jetons qui se sont accumulés en permanence depuis la dernière fois qu'un paquet est arrivé.
3. Le nombre total de jetons cumulés ne peut pas dépasser la valeur maxtokens. Supprimer les jetons excédentaires.
4. Vérifier la conformité des paquets.

La réglementation permet également de limiter les taux. Il s'agit d'un exemple de configuration afin de fournir une limitation de débit sur l'interface Ethernet qui utilise la réglementation basée sur les classes.

```
class-map match-all rtp1
   match ip rtp 2000 10
!
   policy-map p3b
   class rtp1
   police 200000 6250 6250 conform-action transmit exceed-action drop violate-action    drop
policy-map p2
   class rtp1
   police 250000 7750 7750 conform-action transmit exceed-action drop violate-action    drop
   !
interface Ethernet3/0
   service-policy output p3b
   service-policy input p2
```

Cet exemple de sortie de la commande show policy-map interface illustre des valeurs correctement calculées et synchronisées pour les débits et les débits offerts, ainsi que pour les

débits conformes et supérieurs.

```
router#show policy-map interface ethernet 3/0
  Ethernet3/0

   Service-policy input: p2

     Class-map: rtp1 (match-all)
       88325 packets, 11040625 bytes
       30 second offered rate 400000 bps, drop rate 150000 bps
       Match: ip rtp 2000 10
       police:
         250000 bps, 7750 limit, 7750 extended limit
         conformed 55204 packets, 6900500 bytes; action: transmit
         exceeded 33122 packets, 4140250 bytes; action: drop
         conformed 250000 bps, exceed 150000 bps violate 0 bps

       Service-policy : p3b

         Class-map: rtp1 (match-all)
           88325 packets, 11040625 bytes
           30 second offered rate 400000 bps, drop rate 50000 bps
           Match: ip rtp 2000 10
           police:
             200000 bps, 6250 limit, 6250 extended limit
             conformed 44163 packets, 5520375 bytes; action: transmit
             exceeded 11041 packets, 1380125 bytes; action: drop
             conformed 200000 bps, exceed 50000 bps violate 0 bps

         Class-map: class-default (match-any)
           0 packets, 0 bytes
           30 second offered rate 0 bps, drop rate 0 bps
           Match: any
```

Problèmes connus avec le CAR et les compteurs de contrôle de classe

Ce tableau répertorie les problèmes résolus avec les compteurs affichés dans les commandes **show policy-map** ou **show interface rate-limit**. Les clients enregistrés qui sont connectés peuvent afficher les informations de bogue dans l'outil de recherche de bogues.

Symptôme	ID de bogues résolus et solutions de contournement

Compteurs d'abandon inférieurs aux attentes	• ID de bogue Cisco CSCdv41231 (clients enregistrés uniquement)Lorsqu'une stratégie de service hiérarchique d'entrée utilise la commande **police** aux niveaux parent et enfant, le régulateur peut abandonner moins que le nombre de paquets attendu, car le régulateur de niveau parent doit être congestionné avant de supprimer les paquets. Voici un exemple d'une telle politique :
	`policy-map child`
	`class dscp1`
	`police cir 100000 bc 3000 conform-action transmit exceed-action drop`
	`!`

	policy-map parent class rtp1 police cir 250000 bc 7750 conform- action transmit exceed-action drop service-policy child Comme solution de contournement, créez des stratégies distinctes et appliquez-en une en entrée et une en sortie afin d'éviter la configuration d'une stratégie hiérarchique.
Doubler le taux de pertes et de débit attendu	• ID de bogue Cisco CSCds23924 (clients enregistrés uniquement)Cisco Express Forwarding (CEF) définit un mécanisme de commutation IOS qui transfère les paquets de l'interface d'entrée vers l'interface de sortie. Avant les modifications implémentées à partir de cet ID de bogue, les mécanismes CEF et QoS configurés tels que CAR ou la réglementation basée sur les classes incrémentaient les compteurs de paquets. Il en résulte ce que l'on appelle la comptabilité double, des paquets conformés gonflés et des valeurs de perte excédentaires. • ID de bogue Cisco CSCdr40598 (clients enregistrés uniquement)Sur la gamme Cisco 12000, lorsque le CAR de sortie est activé et que la carte de ligne d'entrée est le moteur 2, les compteurs de sortie de sortie sont doublés. Cette double comptabilisation résulte de la manière dont les compteurs de sortie sont gérés. • ID de bogue Cisco CSCdv84259 (clients enregistrés uniquement)Si vous activez globalement la commande **ip cef distribute** sur un routeur de la gamme Cisco 7500, une interface de carte VIP (Versatile Interface Processor) non-Versatile apparaît avec la commande **ip route-cache distribute** activée par défaut. Les non-VIP ne prennent pas en charge le CEF distribué, et un effet secondaire rare de cette commande qui apparaît sur les non-VIP est la double comptabilisation.
Aucune baisse ou un taux de chut	En général, lorsque vous appliquez des fonctions QoS basées sur les classes, la première étape du dépannage consiste à s'assurer que le mécanisme de classification QoS fonctionne correctement. En d'autres termes, assurez-vous que les paquets spécifiés dans les instructions match dans votre class-map atteignent les classes correctes. router#**show policy-map interface** ATM4/0.1

e nul	Service-policy input: drop-inbound-http-hacks (1061) Class-map: http-hacks (match-any) (1063/2) 149 packets, 18663 bytes 5 minute offered rate 2000 bps, drop rate 0 bps Match: protocol http url "*cmd.exe*" (1067) 145 packets, 18313 bytes 5 minute rate 2000 bps Match: protocol http url "*.ida*" (1071) 0 packets, 0 bytes 5 minute rate 0 bps Match: protocol http url "*root.exe*" (1075) 4 packets, 350 bytes 5 minute rate 0 bps Match: protocol http url "*readme.eml*" (1079) 0 packets, 0 bytes 5 minute rate 0 bps police: 1000000 bps, 31250 limit, 31250 extended limit conformed 0 packets, 0 bytes; action: drop exceeded 0 packets, 0 bytes; action: drop violated 0 packets, 0 bytes; action: drop conformed 0 bps, exceed 0 bps violate 0 bps • ID de bogue Cisco CSCds34478 (clients enregistrés uniquement)La classification échoue lorsque CEF, et non DCEF, est activé et qu'une stratégie d'entrée est associée à un circuit virtuel permanent ATM. Dans le logiciel Cisco IOS Version 12.1T, la classification des sorties échoue lorsque CEF, et non DCEF, est activé et qu'une politique de sortie est associée à un circuit virtuel permanent ATM.
Taux de chute anormal ou incohérent	• ID de bogue Cisco CSCdw50583 (clients enregistrés uniquement)Le taux de chute affiché dans la carte-classe ne correspond pas au taux de chute indiqué par l'action de la police. Dans cet exemple de sortie, le taux de chute pour la classe est de 745000 bps, tandis que le taux de chute affiché par l'action de la police est de 1072000 bps. router#**show policy-map interface** Serial3/0.1: DLCI 13 - Service-policy output: out Class-map: c2 (match-all) 172483 packets, 91760956 bytes 30 second offered rate 1384000 bps, drop rate 745000 bps Match: ip precedence 0 police: 384000 bps, 1500 limit, 1500

```
    extended limit
             conformed 38903 packets, 20696396
    bytes; action: transmit
             exceeded 133580 packets, 71064560
    bytes; action: drop
             conformed 311000 bps, exceed 1072000
    bps violate 0 bps
```

Informations connexes

- Configuration du débit d'accès garanti
- Contrôle avec CAR
- Utilisation de CAR lors d'attaques par déni de service (DoS)
- Page d'assistance technologique QoS
- Page d'assistance pour les protocoles de routage IP
- Page de support pour le routage IP
- Support et documentation techniques - Cisco Systems