Quality of Service-Optionen auf GRE-Tunnelschnittstellen

Inhalt

Einführung

In diesem Dokument wird erläutert, welche Quality of Service (QoS)-Funktionen auf Tunnelschnittstellen mithilfe von Generic Routing Encapsulation (GRE) konfiguriert werden können. Mit IP Security (IPsec) konfigurierte Tunnel werden nicht in diesem Dokument behandelt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Überblick über GRE

Bevor Sie sich mit QoS über GRE-Tunnel vertraut machen, müssen Sie zunächst das Format eines getunnelten Pakets verstehen.

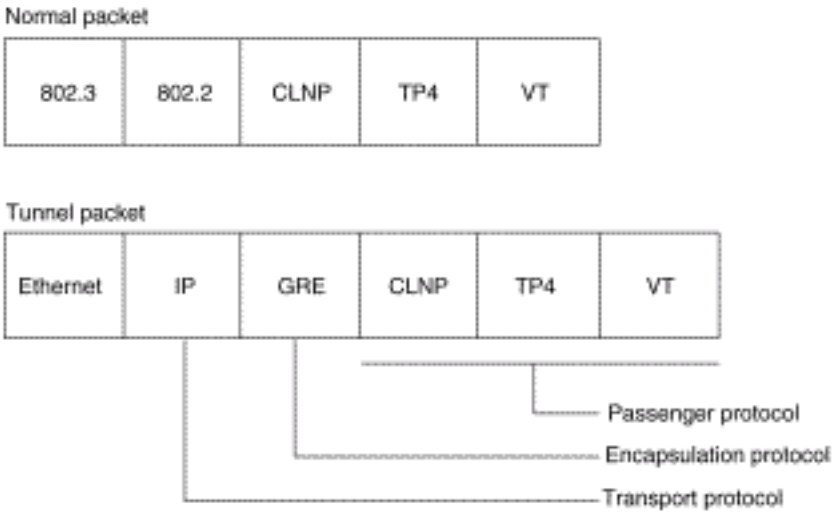
Eine Tunnelschnittstelle ist eine virtuelle oder logische Schnittstelle auf einem Router, auf dem Cisco IOS® Software ausgeführt wird. Es entsteht eine virtuelle Point-to-Point-Verbindung zwischen zwei Cisco Routern an Remote-Punkten über ein IP-Internetwork.

GRE ist ein von IOS unterstütztes und in RFC 1702 definiertes Kapselungsprotokoll. Tunneling-Protokolle kapseln Pakete innerhalb eines Transportprotokolls ein.

Eine Tunnelschnittstelle unterstützt einen Header für jeden der folgenden Bereiche:

- Ein Passagierprotokoll oder ein gekapseltes Protokoll, z. B. IP, AppleTalk, DECnet oder IPX.
- Ein Carrier-Protokoll (in diesem Fall GRE).
- Ein Transportprotokoll (nur in diesem Fall IP).

Das Format eines Tunnelpakets wird hier veranschaulicht:



Weitere Informationen zur Konfiguration von GRE-Tunneln finden Sie unter Konfigurieren logischer Schnittstellen.

Cisco QoS für GRE-Tunnel

Eine Tunnelschnittstelle unterstützt viele der gleichen QoS-Funktionen wie eine physische Schnittstelle. In diesen Abschnitten werden die unterstützten QoS-Funktionen beschrieben.

Shaping

Mit der Cisco IOS Software Release 12.0(7)T wurde die Unterstützung für die Anwendung von GTS (Generic Traffic Shaping) direkt auf die Tunnelschnittstelle eingeführt. In der folgenden Beispielkonfiguration wird die Tunnelschnittstelle in eine Gesamtausgangsrate von 500 Kbit/s umgewandelt. Weitere Informationen finden Sie unter Konfigurieren des allgemeinen Traffic Shaping.

```
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
```

Die Cisco IOS Software, Version 12.1(2)T, bietet jetzt Unterstützung für klassenbasiertes Shaping über die modulare QoS-Kommandozeilenschnittstelle (MQC). In der folgenden Beispielkonfiguration wird veranschaulicht, wie die gleiche Shaping-Richtlinie mit den MQC-Befehlen auf die Tunnelschnittstelle angewendet wird. Weitere Informationen finden Sie unter Konfigurieren von klassenbasiertem Shaping.

```
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
```

Richtlinienvergabe

Wenn eine Schnittstelle überlastet wird und Pakete mit der Warteschlange beginnen, können Sie eine Warteschlangenmethode auf Pakete anwenden, die auf die Übertragung warten. Logische Cisco IOS-Schnittstellen unterstützen keinen Überlastungszustand und unterstützen nicht die direkte Anwendung einer Service-Richtlinie, die eine Warteschlangenmethode anwendet. Stattdessen müssen Sie eine hierarchische Richtlinie wie folgt anwenden:

1. Erstellen Sie eine "untergeordnete" Richtlinie oder eine Richtlinie der unteren Ebene, die einen Warteschlangenmechanismus konfiguriert, z. B. Warteschlangenverwaltung mit niedriger Latenz mit dem **Priority**-Befehl und klassenbasiertes Weighted Fair Queueing (CBWFQ) mit dem **Bandbreitenbefehl**. Weitere Informationen finden Sie unter Überlastungsmanagement.
   ```
   policy-map child
    class voice
     priority 512
   ```
2. Erstellen Sie eine übergeordnete Richtlinie oder eine Richtlinie der obersten Ebene, die klassenbasiertes Shaping anwendet. Wenden Sie die untergeordnete Richtlinie als Befehl unter der übergeordneten Richtlinie an, da die Zugangskontrolle für die untergeordnete Klasse basierend auf der Shaping-Rate für die übergeordnete Klasse erfolgt.
   ```
   policy-map tunnel
    class class-default
     shape average 2000000
     service-policy child
   ```
3. Wenden Sie die übergeordnete Richtlinie auf die Tunnelschnittstelle an.

```
interface tunnel0
   service-policy tunnel
```

Der Router druckt diese Protokollmeldung, wenn eine Tunnelschnittstelle mit einer Dienstrichtlinie konfiguriert ist, die Warteschlangen ohne Shaping anwendet.

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

Tunnelschnittstellen unterstützen auch klassenbasierte Richtlinienvergabe, unterstützen jedoch keine CAR (Committed Access Rate).

Hinweis: Dienstrichtlinien werden auf Tunnelschnittstellen des 7500 nicht unterstützt.

Überlastungsvermeidung

In der Cisco IOS Software-Version 11.3T wurden GRE-Tunnelmarking und DSCP- oder IP-Precedence-Werte eingeführt, die den Router so konfigurieren, dass die IP-Rangfolge-Bit-Werte des ToS-Bytes in den Tunnel oder GRE-IP-Header kopiert werden, der das innere Paket kapselt. Zuvor waren diese Bits auf Null gesetzt. Zwischenrouter zwischen den Tunnelendpunkten können mithilfe der IP-Rangfolgewerte Pakete für QoS-Funktionen wie Richtlinien-Routing, WFQ und WRED (Weighted Random Early Detection) klassifizieren.

Der Befehl QoS-Vorklassifizierung

Wenn Pakete durch Tunnel- oder Verschlüsselungs-Header gekapselt werden, können QoS-Funktionen die ursprünglichen Paket-Header nicht überprüfen und die Pakete nicht korrekt klassifizieren. Pakete, die über denselben Tunnel übertragen werden, haben dieselben Tunnel-Header, sodass die Pakete bei überlasteter physischer Schnittstelle identisch behandelt werden. Mit der Einführung der Funktion Quality of Service for Virtual Private Networks (VPNs) können Pakete jetzt klassifiziert werden, bevor Tunneling und Verschlüsselung stattfinden.

In diesem Beispiel ist tunnel0 der Tunnelname. Der Befehl **QoS-Vorklassifizierung** aktiviert die Funktion QoS für VPNs in Tunnel0:

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

Hinweis: Der Befehl **QoS** zur Vorklassifizierung kann verwendet werden, um Datenverkehr anhand anderer Werte als IP-Rangfolge oder DSCP zu klassifizieren. Sie können beispielsweise Pakete anhand von IP-Fluss- oder Layer-3-Informationen klassifizieren, z. B. Quell- und Ziel-IP-Adresse, für die dieser Befehl verwendet werden kann. Der Befehl **QoS zur Vorklassifizierung** ist nur erforderlich, wenn Sie den Datenverkehr über IP, Protokoll oder Port klassifizieren. Wenn die Klassifizierung auf dem DSCP-Code basiert, ist **QoS-Vorklassifizierung** nicht erforderlich.

Charakterisierung von Datenverkehr für QoS-Richtlinien

Beim Konfigurieren einer Dienstrichtlinie müssen Sie möglicherweise zuerst den Datenverkehr charakterisieren, der den Tunnel durchläuft. Cisco IOS unterstützt Netflow und IP Cisco Express Forwarding (CEF) Accounting auf logischen Schnittstellen wie Tunneln. Weitere Informationen finden Sie im NetFlow Services Solutions Guide.

Wo wende ich die Service-Richtlinie an?

Sie können eine Dienstrichtlinie entweder auf die Tunnelschnittstelle oder auf die zugrunde liegende physische Schnittstelle anwenden. Die Entscheidung, wo die Politik anzuwenden ist, hängt von den QoS-Zielen ab. Es hängt auch davon ab, welchen Header Sie für die Klassifizierung verwenden müssen.

- Wenden Sie die Richtlinie auf die Tunnelschnittstelle an, ohne **QoS-preklassifizieren** zu müssen, wenn Sie Pakete basierend auf dem Pre-Tunnel-Header klassifizieren möchten.
- Wenden Sie die Richtlinie auf die *physische* Schnittstelle an, ohne **QoS vorklassifizieren** zu müssen, wenn Sie Pakete basierend auf dem Post-Tunnel-Header klassifizieren möchten. Darüber hinaus wenden Sie die Richtlinie auf die physische Schnittstelle an, wenn Sie den gesamten Verkehr, der zu einem Tunnel gehört, gestalten oder überwachen möchten. Die physische Schnittstelle unterstützt mehrere Tunnel.
- Wenden Sie die Richtlinie auf eine *physische* Schnittstelle an, und aktivieren Sie **QoS-Preklassify** auf einer Tunnelschnittstelle, wenn Sie Pakete basierend auf dem Pre-Tunnel-Header klassifizieren möchten.

Multipoint-Tunnelschnittstellen

CBWFQ in klassenbasiertem Shaping wird auf einer Multipoint-Schnittstelle nicht unterstützt. Cisco Bug ID CSCds87191 konfiguriert den Router so, dass er bei der Ablehnung der Richtlinie eine Fehlermeldung ausgibt.

Bekannte Probleme

In seltenen Fällen führt die Anwendung einer mit dem **shape-**Befehl konfigurierten Dienstrichtlinie zu einer hohen CPU-Auslastung und Ausrichtungsfehlern. Die CPU-Last wird durch Protokollierung der Ausrichtungsfehler verursacht, die wiederum durch das falsche Festlegen der Ausgabeschnittstelle und der Adjacency-Umschreibinformationen verursacht werden. Dieses Problem betrifft nur Nicht-RSP-Plattformen (Low-End) und -Plattformen, die Partikelbasiertes CEF-Switching verwenden, und wird mithilfe der Cisco Bug-IDs CSCdu4504 und CSCuk30302 behoben. Sie können auch die folgenden Problemumgehungen in Betracht ziehen:

- Ersetzen Sie die GRE-Kapselung durch **Tunnel-Modus ipip**.
- Ersetzen Sie den **shape**-Befehl durch den **polizeilichen** Befehl.
- Konfigurieren Sie das Shaping auf der physischen Schnittstelle, die den Tunnel unterstützt.

Zugehörige Informationen

- Quality of Service für virtuelle private Netzwerke
- Konfigurieren des GRE-Tunnels über Kabel
- QoS-Technologieunterstützung
- Konfigurieren eines GRE-Tunnels über IPSec mit OSPF
- Technischer Support und Dokumentation - Cisco Systems