

Opções de qualidade de serviço em interfaces de túnel GRE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Visão geral de GRE](#)

[Cisco QoS para GRE Tunnels](#)

[Modelagem](#)

[Vigilância](#)

[Evitando congestionamento](#)

[O comando qos pre-classify](#)

[Caracterizando o tráfego para políticas QoS](#)

[Onde aplico a política de serviços?](#)

[Interfaces de túnel multiponto](#)

[Problemas conhecidos](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento analisa quais recursos de Qualidade de Serviço (QoS) podem ser configurados em interfaces de túnel usando o Generic Routing Encapsulation (GRE). Os túneis configurados com Segurança IP (IPsec) estão fora do escopo deste documento.

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

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](#)

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

[Visão geral de GRE](#)

Antes de aprender sobre QoS nos túneis GRE, primeiro é necessário entender o formato de um pacote em túnel.

Uma interface de túnel é uma interface virtual ou lógica de um roteador que executa o Software Cisco IOS®. Ela cria um enlace virtual ponto-a-ponto entre dois Cisco routers em pontos remotos sobre uma inter-rede de IP.

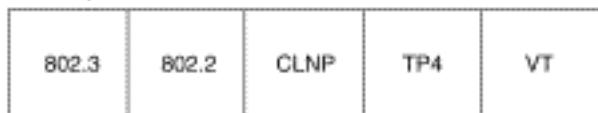
O GRE é um protocolo de encapsulamento suportado pelo IOS e definido no RFC 1702. Os protocolos de tunelamento encapsulam pacotes dentro de um protocolo de transporte.

Uma interface de túnel suporta um cabeçalho para cada um destes:

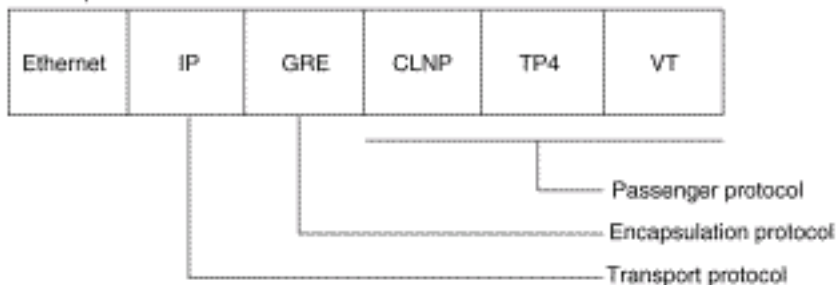
- Um protocolo passageiro ou encapsulado, como IP, AppleTalk, DECnet ou IPX.
- Um protocolo de portadora (GRE, neste caso).
- Um protocolo de transporte (neste caso, somente IP).

O formato de um pacote de túnel está ilustrado aqui:

Normal packet



Tunnel packet



Consulte [Configurando Interfaces Lógicas](#) para obter mais informações sobre como configurar túneis GRE.

[Cisco QoS para GRE Tunnels](#)

Uma interface de túnel suporta diversos dos mesmos recursos de QoS que uma interface física. Estas seções descrevem os recursos de QoS suportados.

[Modelagem](#)

O Cisco IOS Software Release 12.0(7)T introduziu suporte para aplicar a modelagem de tráfego genérico (GTS) diretamente na interface do túnel. O exemplo de configuração a seguir molda a interface de túnel em uma taxa de saída geral de 500 kbps. Consulte [Configuração da Modelagem de Tráfego Genérico](#) para obter mais informações.

```
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
```

O Cisco IOS Software Release 12.1(2)T adicionou suporte para modelagem baseada em classe usando a interface de linha de comando (MQC) de QoS modular. O exemplo de configuração a seguir mostra como aplicar a mesma política de modelagem à interface do túnel com os comandos MQC. Consulte [Configuração da Modelagem Baseada em Classe](#) para obter mais informações.

```
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
```

[Vigilância](#)

Quando uma interface torna-se congestionada e os pacotes entram na fila, é possível aplicar um método de enfileiramento para os pacotes que estão aguardando transmissão. As interfaces lógicas de Cisco IOS não suportam de forma inerente um estado de congestionamento e não suportam a aplicação direta de uma política de serviço que aplica um método de enfileiramento. Em vez disso, você precisa aplicar uma [política hierárquica](#) da seguinte maneira:

1. Crie uma "política infantil" ou uma política de nível mais baixo que configure um mecanismo de enfileiramento, como o enfileiramento de baixa latência com o comando `priority` e o enfileiramento CBWFQ com o comando `bandwidth`. Consulte [Gerenciamento de Congestionamento](#) para obter mais informações.

```
policy-map child
  class voice
    priority 512
```

2. Crie uma política principal ou de alto nível com aplicação de molde com base em classe. Aplique a política filho como um comando sob a política pai, já que o controle de admissão para a classe filho é feito com base na taxa de modelagem para a classe pai.

```
policy-map tunnel
  class class-default
    shape average 2000000
    service-policy child
```

3. Aplique a política pai à interface de túnel.

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

O roteador imprime essa mensagem de log quando uma interface de túnel é configurada com uma política de serviço que aplica o enfileiramento sem modelagem.

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

As interfaces de túnel também suportam [policiamento baseado em classe](#), mas não suportam taxa de acesso comprometida (CAR).

Observação: as políticas de serviço não são suportadas em interfaces de túnel no 7500.

[Evitando congestionamento](#)

O Cisco IOS Software Release 11.3T introduziu a [Marcação de Túnel GRE e os Valores de Precedência DSCP ou IP](#), que configura o roteador para copiar os valores de bit de precedência IP do byte ToS para o túnel ou cabeçalho IP GRE que encapsula o pacote interno. Anteriormente, esses bits estavam definidos como zero. Os roteadores intermediários entre os pontos finais do túnel podem usar os valores de precedência do IP a fim de classificar os pacotes para os recursos de QoS, como o Policy Routing, o WFQ e o Weighted Random Early Detection (WRED).

[O comando qos pre-classify](#)

Quando pacotes são encapsulados por cabeçalhos de túnel ou criptografia, os recursos de QoS não conseguem examinar os cabeçalhos originais dos pacotes nem classificar corretamente os pacotes. Os pacotes que percorrem o mesmo túnel possuem os mesmos cabeçalhos e por isso são tratados de forma idêntica quando a interface física está congestionada. Com a introdução do recurso VPNs (Qualidade de Serviço para Redes Virtuais Privadas), agora os pacotes podem ser classificados antes que ocorra o tunelamento e a criptografia.

Neste exemplo, tunnel0 é o nome do túnel. O comando qos pre-classify habilita o recurso QoS para VPNs em tunnel0:

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

Observação: o comando **qos pre-classify** pode ser usado para classificar o tráfego com base em valores diferentes de precedência de IP ou DSCP. Por exemplo, você pode querer classificar pacotes com base no fluxo IP ou nas informações da Camada 3, como o endereço IP de origem e de destino para os quais esse comando pode ser usado. O comando **qos pre-classify** é necessário somente se você classificar o tráfego em IP, protocolo ou porta. Se a classificação for baseada no código DSCP, então **qos pre-classify** não será necessário.

[Caracterizando o tráfego para políticas QoS](#)

Ao configurar uma política de serviço, você pode primeiro precisar caracterizar o tráfego que está atravessando o túnel. O Cisco IOS dá suporte à contabilização do Netflow e IP Cisco Express Forwarding (CEF) nas interfaces lógicas como túneis. Consulte o [NetFlow Services Solutions Guide](#) para obter mais informações.

[Onde aplico a política de serviços?](#)

É possível aplicar uma política de serviço à interface do túnel ou à interface física subjacente. A

decisão de onde aplicar a política depende dos objetivos de QoS. Isso depende também de qual cabeçalho você precisa usar para classificação.

- Aplique a política à interface de túnel sem `qos-preclassify` se desejar classificar os pacotes com base no cabeçalho pré-túnel.
- Aplique a política à interface *física* sem `qos-preclassify` quando quiser classificar pacotes com base no cabeçalho pós-túnel. Além disso, aplique a política à interface física quando você quiser modelar ou vigiar todo o tráfego pertencente a um túnel e a interface física suportar diversos túneis.
- Aplique a política a uma interface *física* e ative `qos-preclassify` em uma interface de túnel quando quiser classificar pacotes com base no cabeçalho pré-túnel.

Interfaces de túnel multiponto

A modelagem interna com base em classe CBWFQ não é suportada em uma interface multiponto. A identificação de bug Cisco CSCds87191 configura o roteador para imprimir uma mensagem de erro quando rejeitar a política.

Problemas conhecidos

Em condições raras, a aplicação de uma política de serviço configurada com o comando **shape** leva a erros elevados de utilização da CPU e de alinhamento. A carga da CPU é causada pelo registro dos erros de alinhamento, que, por sua vez, são causados pela configuração incorreta do CEF na interface de saída e nas informações de regravação de adjacência. Esse problema afeta somente as plataformas não-RSP (de extremidade baixa) e as plataformas que utilizam switching CEF baseada em partícula. O problema é resolvido via identificações de erro Cisco CSCdu45504 e CSCuk30302. Você também pode considerar estas soluções alternativas:

- Substitua o encapsulamento do GRE por um tunnel mode ipip.
- Substitua o comando `shape` pelo comando `police`.
- Configure a modelagem da interface física que suporta o túnel.

Informações Relacionadas

- [Qualidade de Serviço para redes privadas virtuais](#)
- [Configuração de Túnel GRE no Cabo](#)
- [Suporte da tecnologia de QoS](#)
- [Configurando um Túnel GRE via IPSec com OSPF](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)