

Opzioni Quality of Service sulle interfacce tunnel GRE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Panoramica di GRE](#)

[Cisco QoS per tunnel GRE](#)

[Traffic shaping](#)

[Traffic policing](#)

[Prevenzione delle congestioni](#)

[Il comando qos pre-classify](#)

[Caratterizzazione del traffico per i criteri QoS](#)

[Dove si applica la policy sui servizi?](#)

[Interfacce tunnel Multipoint](#)

[Problemi noti](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene esaminato quali funzionalità QoS (Quality of Service) possono essere configurate sulle interfacce tunnel utilizzando il GRE (Generic Routing Encapsulation). I tunnel configurati con IP Security (IPsec) non sono inclusi nell'ambito di questo documento.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Panoramica di GRE

Prima di conoscere le funzionalità QoS sui tunnel GRE, è necessario comprendere il formato di un pacchetto con tunnel.

L'interfaccia del tunnel è un'interfaccia virtuale o logica usata sui router con software Cisco IOS®. Crea un collegamento virtuale point-to-point tra due router Cisco in punti remoti su una rete IP.

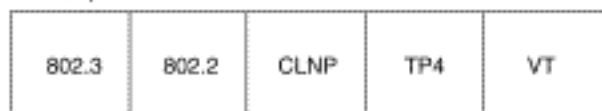
GRE è un protocollo di incapsulamento supportato da IOS e definito nella [RFC 1702](#). I protocolli di tunneling incapsulano i pacchetti all'interno di un protocollo di trasporto.

L'interfaccia del tunnel supporta un'intestazione per ciascuno di questi elementi:

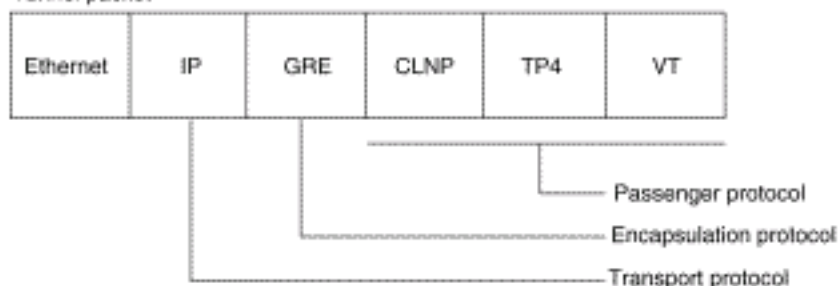
- Protocollo passeggeri o protocollo incapsulato, ad esempio IP, AppleTalk, DECnet o IPX.
- Un protocollo vettore (GRE, in questo caso).
- Un protocollo di trasporto (IP solo in questo caso).

Di seguito è illustrato il formato di un pacchetto del tunnel:

Normal packet



Tunnel packet



Per ulteriori informazioni sulla configurazione dei tunnel GRE, fare riferimento a [Configurazione delle interfacce logiche](#).

Cisco QoS per tunnel GRE

Un'interfaccia tunnel supporta molte delle stesse funzionalità QoS di un'interfaccia fisica. Nelle sezioni seguenti vengono descritte le funzionalità QoS supportate.

Traffic shaping

Il software Cisco IOS versione 12.0(7)T ha introdotto il supporto per l'applicazione del GTS (Generic Traffic Shaping) direttamente sull'interfaccia del tunnel. La seguente configurazione di esempio forma l'interfaccia del tunnel a una velocità di output complessiva di 500 kbps. per ulteriori informazioni, fare riferimento a [Configurazione di Traffic Shaping generico](#).

```
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
```

Nel software Cisco IOS versione 12.1(2)T, è stato aggiunto il supporto per il class-based shaping con l'interfaccia della riga di comando (MQC) QoS modulare. Nella configurazione di esempio seguente viene illustrato come applicare lo stesso criterio di shaping all'interfaccia del tunnel con i comandi MQC. Per ulteriori informazioni, fare riferimento a [Configurazione di Class-Based 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
```

[Traffic policing](#)

Quando un'interfaccia è congestionata e i pacchetti iniziano a entrare in coda, è possibile applicare un metodo di coda ai pacchetti in attesa di essere trasmessi. Le interfacce logiche Cisco IOS non supportano intrinsecamente uno stato di congestione e non supportano l'applicazione diretta di criteri del servizio che applicano un metodo di coda. È invece necessario applicare un [criterio gerarchico](#) come indicato di seguito:

1. Creare un criterio "figlio" o di livello inferiore che configuri un meccanismo di coda, ad esempio l'accodamento a bassa latenza con il comando **priority** e il CBWFQ (Weighted Fair Queueing) basato su classi con il comando **bandwidth**. Per ulteriori informazioni, fare riferimento a [Gestione congestione](#).

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

2. Creare un criterio "padre" o di livello superiore che applichi il shaping basato su classi. Applicare il criterio figlio come comando nel criterio padre poiché il controllo dell'ammissione per la classe figlio viene eseguito in base alla velocità di shaping per la classe padre.

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

3. Applica il criterio padre all'interfaccia del tunnel.

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

Il router stampa questo messaggio di registro quando un'interfaccia del tunnel è configurata con un criterio di servizio che applica l'accodamento senza modifica della forma.

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

Anche le interfacce tunnel supportano il [policing basato su classi](#), ma non supportano il commit access rate (CAR).

Nota: i criteri di servizio non sono supportati sulle interfacce tunnel su 7500.

[Prevenzione delle congestioni](#)

Nel software Cisco IOS versione 11.3T sono stati introdotti i [valori di contrassegno del tunnel GRE e i valori DSCP o IP Precedence](#), per configurare il router in modo da copiare i valori di bit di IP Precedence del byte ToS nell'intestazione tunnel o GRE IP che incapsula il pacchetto interno. In precedenza, questi bit erano impostati su zero. I router intermedi tra gli endpoint del tunnel possono usare i valori di precedenza IP per classificare i pacchetti per le funzionalità QoS, ad esempio routing delle policy, WFQ e WRED (Weighted Random Early Detection).

[Il comando qos pre-classify](#)

Quando i pacchetti sono incapsulati dalle intestazioni del tunnel o dalla crittografia, le funzionalità QoS non sono in grado di esaminare le intestazioni originali dei pacchetti e di classificarli correttamente. I pacchetti che viaggiano attraverso lo stesso tunnel hanno le stesse intestazioni del tunnel, quindi i pacchetti vengono trattati allo stesso modo se l'interfaccia fisica è congestionata. Con l'introduzione della funzionalità [Quality of Service for Virtual Private Network \(VPN\)](#), i pacchetti possono essere classificati prima del tunneling e della crittografia.

Nell'esempio, il nome del tunnel è tunnel0. Il comando **qos pre-classify** abilita la funzionalità QoS per VPN su tunnel0:

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

Nota: Il comando **qos pre-classify** può essere usato per classificare il traffico in base a valori diversi da IP precedence o DSCP. Ad esempio, è possibile classificare i pacchetti in base alle informazioni sul flusso IP o sul layer 3, come l'indirizzo IP di origine e di destinazione per cui è possibile utilizzare questo comando. Il comando **qos pre-classify** è richiesto solo se si classifica il traffico su IP, protocollo o porta. Se la classificazione è basata sul codice DSCP, la **preclassificazione qos** non è necessaria.

[Caratterizzazione del traffico per i criteri QoS](#)

Quando si configura un criterio del servizio, può essere necessario innanzitutto caratterizzare il traffico che attraversa il tunnel. Cisco IOS supporta l'accounting Netflow e IP Cisco Express Forwarding (CEF) su interfacce logiche come i tunnel. Per ulteriori informazioni, consultare la [NetFlow Services Solutions Guide](#).

[Dove si applica la policy sui servizi?](#)

È possibile applicare un criterio del servizio all'interfaccia del tunnel o all'interfaccia fisica

sottostante. La decisione su dove applicare la politica dipende dagli obiettivi QoS. Dipende inoltre dall'instestazione da utilizzare per la classificazione.

- Applicare il criterio all'interfaccia del tunnel senza **preclassificazione qos** quando si desidera classificare i pacchetti in base all'instestazione pre-tunnel.
- Applicare il criterio all'interfaccia *fisica* senza **preclassificazione qos** quando si desidera classificare i pacchetti in base all'instestazione post-tunnel. Inoltre, applicare il criterio all'interfaccia fisica quando si desidera modellare o controllare tutto il traffico appartenente a un tunnel e l'interfaccia fisica supporta diversi tunnel.
- Applicare il criterio a un'interfaccia *fisica* e abilitare la **preclassificazione qos** su un'interfaccia tunnel quando si desidera classificare i pacchetti in base all'instestazione pre-tunnel.

Interfacce tunnel Multipoint

CBWFQ all'interno di class-based shaping non supportato in un'interfaccia multipunto. L'ID bug Cisco [CSCds87191](#) configura il router in modo che stampi un messaggio di errore quando rifiuta il criterio.

Problemi noti

In rari casi, l'applicazione di criteri del servizio configurati con il comando **shape** causa un elevato utilizzo della CPU e errori di allineamento. Il carico della CPU è causato dalla registrazione degli errori di allineamento, che a loro volta sono causati da CEF che imposta in modo errato l'interfaccia di output e le informazioni di riscrittura adiacenti. Questo problema interessa solo le piattaforme non RSP (low-end) e le piattaforme che utilizzano la commutazione CEF basata su particelle ed è risolto tramite gli ID bug Cisco [CSCdu45504](#) e [CSCuk30302](#). Per risolvere il problema, considerare anche le seguenti soluzioni:

- Sostituire l'incapsulamento GRE con l'ipp **della modalità tunnel**.
- Sostituire il comando **shape** con il comando **Police**.
- Configurare il shaping sull'interfaccia fisica che supporta il tunnel.

Informazioni correlate

- [Quality of Service per reti private virtuali](#)
- [Configurazione del tunnel GRE sul cavo](#)
- [Supporto tecnologia QoS](#)
- [Configurazione di un tunnel GRE su IPSec con OSPF](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)