# GRE 터널 인터페이스의 서비스 품질 옵션

## 목차



## 소개

이 문서에서는 GRE(Generic Routing Encapsulation)를 사용하여 터널 인터페이스에서 구성할 수 있는 QoS(Quality of Service) 기능을 검토합니다. IPsec(IP Security)으로 구성된 터널은 이 문서의 범위를 벗어납니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

# GRE 개요

GRE 터널을 통해 QoS에 대해 알아보기 전에 먼저 터널링된 패킷의 형식을 이해해야 합니다.

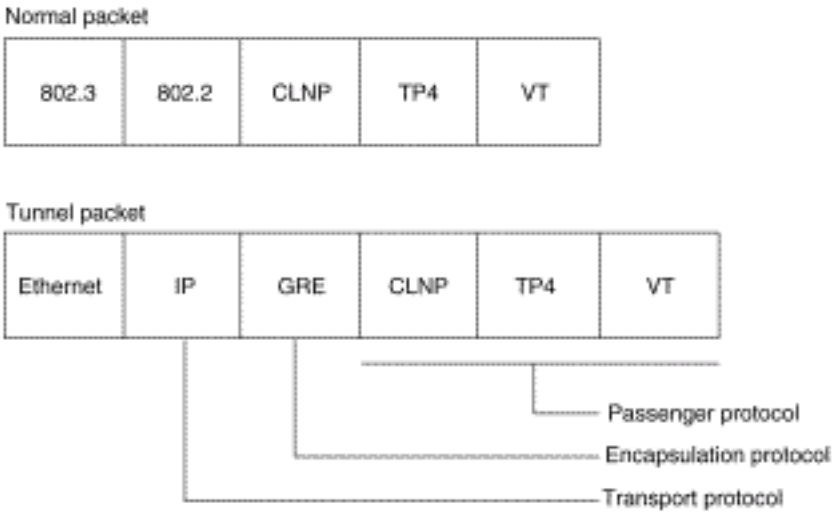
터널 인터페이스는 Cisco IOS® 소프트웨어를 실행하는 라우터의 가상 또는 논리적 인터페이스입니다.IP 인터네트워크를 통해 원격 지점에 있는 두 Cisco 라우터 간에 가상 포인트 투 포인트 링크를 생성합니다.

GRE는 IOS에서 지원되고 RFC 1702에 정의된 캡슐화 프로토콜입니다 .터널링 프로토콜은 전송 프로토콜 내부에 패킷을 캡슐화합니다.

터널 인터페이스는 다음 각 항목에 대한 헤더를 지원합니다.

- IP, AppleTalk, DECnet 또는 IPX와 같은 승객 프로토콜 또는 캡슐화된 프로토콜.
- 캐리어 프로토콜(이 경우 GRE).
- 전송 프로토콜(이 경우 IP만 해당).

터널 패킷의 형식은 다음과 같습니다.




GRE 터널 구성에 대한 자세한 내용은 논리적 인터페이스 구성을 참조하십시오.

# GRE 터널용 Cisco QoS

터널 인터페이스는 물리적 인터페이스와 동일한 여러 QoS 기능을 지원합니다.이 섹션에서는 지원되는 QoS 기능에 대해 설명합니다.

## 셰이핑

Cisco IOS Software Release12.0(7)T는 터널 인터페이스에 직접 GTS(generic traffic shaping)를 적용하는 지원을 도입했습니다.다음 샘플 컨피그레이션은 터널 인터페이스를 전체 출력 속도 500kbps로 구성합니다.자세한 내용은 일반 트래픽 셰이핑 구성을 참조하십시오.

```
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
```

Cisco IOS Software 릴리스 12.1(2)T는 모듈형 QoS MQC(Command-Line Interface)를 사용하여 클래스 기반 셰이핑을 지원합니다. 다음 샘플 컨피그레이션에서는 MQC 명령을 사용하여 터널 인터페이스에 동일한 쉐이핑 정책을 적용하는 방법을 보여줍니다.자세한 내용은 클래스 기반 셰이핑 구성을 참조하십시오.

```
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
```

## 폴리싱

인터페이스가 혼잡해지고 패킷이 대기열로 시작되면 전송 대기 중인 패킷에 대기 방법을 적용할 수 있습니다.Cisco IOS 논리적 인터페이스는 기본적으로 혼잡 상태를 지원하지 않으며 대기열 지정 방법을 적용하는 서비스 정책의 직접 적용을 지원하지 않습니다.대신 다음과 같이 계층적 정책을 적용해야 합니다.

1. priority 명령을 사용하여 낮은 레이턴시 대기열 처리 및 **bandwidth** 명령을 사용하여 클래스 기반 CBWFQ(Weighted Fair Queuing)와 같이 대기열 처리 메커니즘을 구성하는 "하위" 또는 하위 레벨 정책을 생성합니다.자세한 내용은 혼잡 관리를 참조하십시오.
   ```
   policy-map child
    class voice
     priority 512
   ```
2. 클래스 기반 셰이핑을 적용하는 "상위" 또는 최상위 정책을 생성합니다.자식 클래스에 대한 허용 제어는 부모 클래스의 쉐이핑 속도를 기반으로 하므로 자식 정책을 부모 정책 아래의 명령으로 적용합니다.
   ```
   policy-map tunnel
    class class-default
     shape average 2000000
     service-policy child
   ```
3. 터널 인터페이스에 상위 정책을 적용합니다.
   ```
   interface tunnel0
      service-policy tunnel
   ```

라우터는 셰이핑 없이 큐잉을 적용하는 서비스 정책으로 터널 인터페이스가 구성된 경우 이 로그 메시지를 인쇄합니다.

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

터널 인터페이스도 클래스 기반 폴리싱을 지원하지만 CAR(Committed Access Rate)을 지원하지 않습니다.

**참고:** 서비스 정책은 7500의 터널 인터페이스에서 지원되지 않습니다.

## 혼잡 방지

Cisco IOS Software Release 11.3T는 내부 패킷을 캡슐화하는 터널 또는 GRE IP 헤더에 ToS 바이트의 IP 우선순위 비트 값을 복사하도록 라우터를 구성하는 GRE Tunnel Marking 및 DSCP 또는 IP Precedence Values를 도입했습니다.이전에는 이러한 비트가 0으로 설정되었습니다.터널 엔드포인트 간의 중간 라우터는 IP 우선순위 값을 사용하여 정책 라우팅, WFQ, WRED(Weighted Random Early Detection) 등의 QoS 기능에 대한 패킷을 분류할 수 있습니다.

### qos pre-classify 명령

패킷이 터널 또는 암호화 헤더로 캡슐화될 경우 QoS 기능은 원래 패킷 헤더를 검사하고 패킷을 올바르게 분류할 수 없습니다.동일한 터널을 통과하는 패킷은 동일한 터널 헤더를 가지므로 물리적 인터페이스가 혼잡할 경우 패킷이 동일하게 처리됩니다.VPN(Quality of Service for Virtual Private Networks) 기능을 도입하여 터널링 및 암호화가 발생하기 전에 패킷을 분류할 수 있습니다.

이 예에서 tunnel0은 터널 이름입니다.qos **pre-classify** 명령은 tunnel0에서 VPN에 대한 QoS 기능을 활성화합니다.

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

**참고:** qos **pre-classify** 명령을 사용하여 IP 우선 순위 또는 DSCP 이외의 값을 기준으로 트래픽을 분류할 수 있습니다.예를 들어, 이 명령을 사용할 수 있는 소스 및 대상 IP 주소와 같은 IP 흐름 또는 레이어 3 정보를 기반으로 패킷을 분류할 수 있습니다.qos **pre-classify** 명령은 IP, 프로토콜 또는 포트에서 트래픽을 분류하는 경우에만 필요합니다.분류가 DSCP 코드를 기반으로 하는 경우 **qos 사전 분류가** 필요하지 않습니다.

## QoS 정책에 대한 트래픽 특성 지정

서비스 정책을 구성할 때 먼저 터널을 통과하는 트래픽의 특성을 지정해야 할 수 있습니다.Cisco IOS는 터널과 같은 논리적 인터페이스에서 Netflow 및 IP Cisco CEF(Express Forwarding) 어카운팅을 지원합니다.자세한 내용은 NetFlow 서비스 솔루션 가이드를 참조하십시오.

## 서비스 정책은 어디에서 적용합니까?

터널 인터페이스 또는 기본 물리적 인터페이스에 서비스 정책을 적용할 수 있습니다.정책을 적용할 위치의 결정은 QoS 목표에 따라 달라집니다.또한 분류에 사용해야 하는 헤더에 따라 달라집니다.

- 사전 터널 헤더를 기반으로 패킷을 분류하려는 경우 qos-**preclassify** 없이 터널 인터페이스에 정책을 적용합니다.
- 포스트 터널 헤더를 기반으로 패킷을 분류하려는 경우 qos-**preclassify**가 없는 *물리적* 인터페이스에 정책을 적용합니다.또한 터널에 속하는 모든 트래픽을 셰이핑하거나 폴리싱하려면 물리적 인터페이스에 정책을 적용하고, 물리적 인터페이스는 여러 터널을 지원합니다.
- 사전 터널 헤더를 기반으로 패킷을 분류하려는 경우 *물리적* 인터페이스**에** 정책을 적용하고 터널 인터페이스에서 qos-preclassify를 활성화합니다.

## 멀티포인트 터널 인터페이스

CBWFQ 내부 클래스 기반 셰이핑은 다중 지점 인터페이스에서 지원되지 않습니다.Cisco 버그 ID CSCds87191은 정책을 거부할 때 오류 메시지를 인쇄하도록 라우터를 구성합니다.

## 알려진 문제

드문 경우이지만 shape 명령으로 구성된 서비스 정책을 적용하면 CPU 사용률 및 정렬 오류가 증가합니다.CPU 부하는 정렬 오류를 로깅함으로써 발생하며, 이는 CEF가 출력 인터페이스 및 인접성 재작성 정보를 잘못 설정했기 때문입니다.이 문제는 입자 기반 CEF 스위칭을 사용하는 비RSP 플랫폼(로우엔드) 및 플랫폼에만 영향을 미치며 Cisco 버그 ID CSCdu45504 및 CSCuk30302를 통해 해결됩니다. 다음 해결 방법도 고려할 수 있습니다.

- GRE 캡슐화를 **터널 모드 ipip로 대체합니다**.
- **shape** 명령을 **police** 명령으로 대체합니다.
- 터널을 지원하는 물리적 인터페이스에서 셰이핑을 구성합니다.

## 관련 정보

- 가상 사설 네트워크의 QoS(Quality of Service)
- 케이블을 통한 GRE 터널 구성
- QoS 기술 지원
- OSPF를 사용하여 IPSec을 통한 GRE 터널 구성
- 기술 지원 및 문서 – Cisco Systems