

IP Precedence for GRE Tunnels

Feature Summary

Prior to this feature, at generic route encapsulation-based tunnel endpoints, the Type of Service (TOS) bits (including precedence bits) were not copied to the tunnel or GRE IP header that encapsulates the inner packet. Instead, those bits were set to zero. This was not a problem unless the intermediate routers between two tunnel endpoints honored TOS or precedence bits, in which case those settings were ignored.

With the advent of virtual private network (VPN) and QoS applications, it is desirable to copy the TOS bits when the router encapsulates the packets using GRE. Thus, intermediate routers between tunnel endpoints can take advantage of the QoS features such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

Benefits

This feature provides the following benefits:

- Routers between GRE tunnel endpoints will adhere to precedence bits and other TOS bits, thereby possibly improving the routing of important packets. Cisco IOS Quality-of-Service technology, such as policy routing, Committed Access Rate, WFQ, and WRED can operate on intermediate routers between GRE tunnel endpoints.
- Additional security is possible when Cisco IOS network layer encryption is used with precedence for GRE tunnels to provide data confidentiality between VPN tunnel endpoints.
- QoS policy granularity is available per network, per user, and per application.
- The deployment of a GRE tunnel is flexible; it can be applied at the Enterprise CPE or at the Service Provider ingress point.

Restrictions

This feature applies to GRE tunnels only.

Platforms

This feature is supported on all Cisco platforms that Cisco IOS Release 11.3T supports.

Configuration Tasks

None; this feature occurs by default.

Command Reference

None.