QoS on Ethernet over GRE Tunnels

The QoS on Ethernet over GRE (EoGRE) Tunnels feature enables service providers to configure one common Quality of Service (QoS) policy for all endpoints, where an end-point can be a customer premise equipment (CPE) or a VLAN on a CPE. This feature supports high availability on a route processor.

- Finding Feature Information, on page 1
- Restrictions for QoS on Ethernet over GRE Tunnels, on page 1
- Information About QoS on Ethernet over GRE Tunnels, on page 2
- Scaling Considerations for QoS on Ethernet over GRE Tunnels, on page 4
- How to Configure QoS on Ethernet over GRE Tunnels, on page 4
- Configuration Examples for QoS on Ethernet over GRE Tunnels, on page 8
- Additional References, on page 9
- Feature Information for QoS on Ethernet over GRE Tunnels, on page 10

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for QoS on Ethernet over GRE Tunnels

- Per-session QoS policies are not supported in conjunction with the tunnel QoS (class-default policer).
- The QoS policy can be applied for an entire tunnel, but not per-virtual local area network (VLAN) and per-customer premises equipment (CPE).
- Upstream QoS for EoGRE tunnel is not supported.
- Hierarchical QoS, bandwidth guarantees, priority, and shaping are not supported.
- Dynamic per-endpoint QoS policies downloaded from the authentication, authorization, and accounting (AAA) server are not supported.

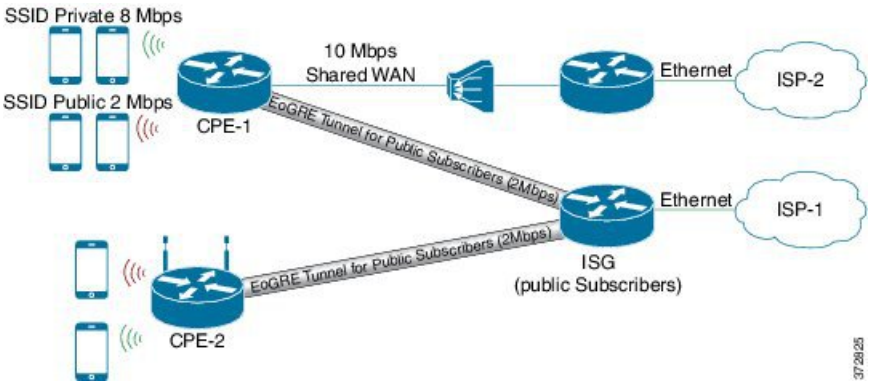
Information About QoS on Ethernet over GRE Tunnels

EoGRE Downstream QoS

The Quality of Service (QoS) on Ethernet over GRE (EoGRE) Tunnels feature enables service providers to apply a unified QoS policy on all endpoints of a tunnel. This controls the bandwidth that public subscribers can download and ensures maximum bandwidth for private customers.

In the deployment scenario given in the figure below, the total available WAN bandwidth at the customer premise equipment (CPE) is 10 Mbps, of which public users are allowed 2 Mbps and the remaining bandwidth is available for private users.

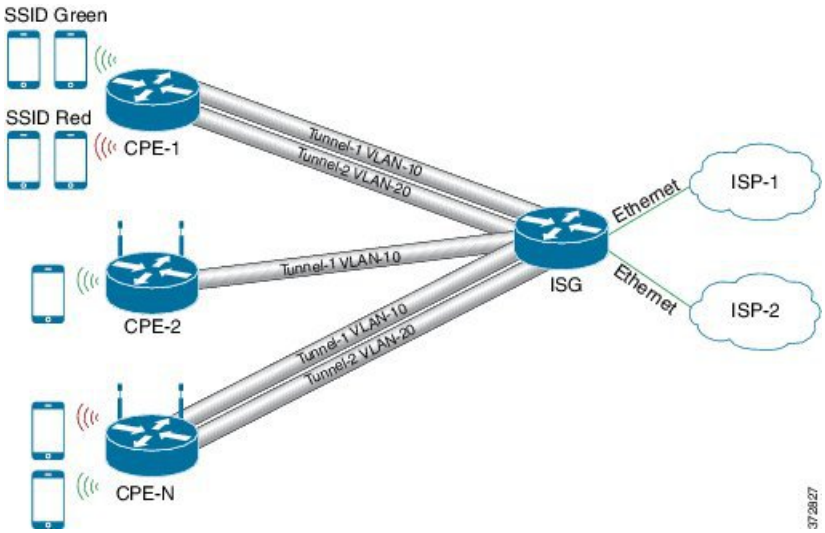
Figure 1: EoGRE Downstream QoS Use Case



Single SSID

Mobile nodes connect to wireless access points (APs). These APs have Service Set Identifiers (SSIDs) provided by the service provider. The SSID of a customer premise equipment (CPE) is the VLAN identifier. Service providers can provide more than one public SSID at a CPE. If a CPE has more than one SSID, then additional mGRE tunnels are configured with a corresponding VLAN tag. The configured multipoint generic routing encapsulation (mGRE) tunnels learn about remote subscribers and the corresponding CPEs independently. This ensures that VLANs, their subnets, default gateways, and VRFs are kept separate and independent of each other, and any QoS policy that is configured on each endpoint of these tunnels also applies to the traffic from the VLAN on the CPE.

Figure 2: Separate Tunnels for Each SSID



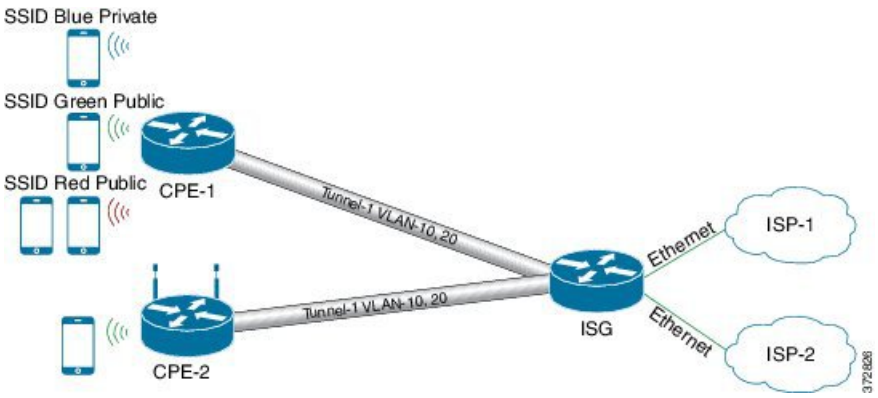
Multiple SSIDs

In a single tunnel for a multiple Service Set Identifiers (SSID), service providers can configure a VLAN range on the multipoint generic routing encapsulation (mGRE) tunnel. When a subscriber traffic is received, the traffic is matched according to the tunnel source and the VLAN range. The Ethernet over GRE (EoGRE) control process also learns the MAC address of subscribers and the VLAN tag of the CPE from which the traffic is originating.

Note You cannot change a VLAN configuration if any subscriber session or MAC address is already learned in the EoGRE control process. To change the VLAN configurations, you must clear all subscriber sessions.

In the figure below, all endpoints learned on Tunnel-1 represent a CPE and a Quality of Service (QoS) policy applied on this tunnel endpoint applies to all traffic going towards the CPE irrespective of the VLAN.

Figure 3: Single Tunnel for Multiple SSIDs



Scaling Considerations for QoS on Ethernet over GRE Tunnels

QoS on EoGRE tunnels support the following scaling features for ESP40, ESP100 and ESP200:

- 64 k EoGREv4 Transport Tunnels, 1 VLAN, 1 Subscriber per Tunnel
- 32 k EoGREv4 Transport Tunnels, 2 VLANs, 2 Subscribers per Tunnel
- 64 k EoGREv4 Transport Tunnels, 1 VLAN, 1 Subscriber per Tunnel, ISG as DHCP relay

How to Configure QoS on Ethernet over GRE Tunnels

Configuring Downstream QoS Policy on Ethernet over GRE Tunnels

Before you begin

Create a Quality of Service (QoS) policy map to attach to the Ethernet over GRE (EoGRE) tunnel.

Note How to create a QoS policy map is not described in the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **interface source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
5. **tunnel vlan** *vlan-id*
6. **ip address** *ip-address mask*
7. **tunnel mode ethernet gre** {**ipv4** | **ipv6**}
8. **tunnel endpoint service-policy output** *policy-map-name*
9. **ip subscriber l2-connected**
10. **initiator unclassified mac-address**
11. **initiator dhcp**
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *tunnel-number* **Example:** `Device(config)# interface tunnel 1`	Specifies a tunnel interface and number and enters interface configuration mode.
Step 4	**interface source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} **Example:** `Device(config-if)# tunnel source loopback 2`	Sets the source address of a tunnel interface.
Step 5	**tunnel vlan** *vlan-id* **Example:** `Device(config-if)# tunnel vlan 10, 20`	Associates a VLAN identifier with the Ethernet over GRE tunnel.
Step 6	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.4.3 255.255.255.0`	Specifies the IP address and mask of the mobile node.
Step 7	**tunnel mode ethernet gre** {**ipv4** | **ipv6**} **Example:** `Device(config-if)# tunnel mode ethernet gre ipv4`	Sets the encapsulation mode of the tunnel to Ethernet over GRE IPv4 or GRE IPv6.
Step 8	**tunnel endpoint service-policy output** *policy-map-name* **Example:** `Device(config-if)# tunnel endpoint service-policy output tunnel-qos-policy`	Configures the QoS policy for tunnel endpoints.
Step 9	**ip subscriber l2-connected** **Example:** `Device(config-if)# ip subscriber l2-connected`	Enters IP subscriber configuration mode.
Step 10	**initiator unclassified mac-address** **Example:** `Device(config-subscriber)# initiator unclassified mac-address`	Initiates IP sessions from unclassified MAC address.
Step 11	**initiator dhcp** **Example:** `Device(config-subscriber)# initiator dhcp`	Enables IP sessions initiated by DHCP.

	Command or Action	Purpose
Step 12	**end** **Example:** `Device(config-subscriber)# end`	Exits to global configuration mode.

Verifying QoS on Ethernet over GRE Tunnels

The **show** commands can be entered in any order.

Before you begin

Configure QoS on Ethernet over GRE (EoGRE) tunnel.

SUMMARY STEPS

1. **show interface tunnel** *tunnel-interface*
2. **show tunnel endpoints tunnel** *tunnel-interface*
3. **show tunnel mac-table tunnel** *tunnel-interface*
4. **show policy-map multipoint tunnel** *tunnel-interface*

DETAILED STEPS

Step 1 **show interface tunnel** *tunnel-interface*

This command displays information about the tunnel.

Example:

```
Device# show interface tunnel 1

Tunnel1 is up, line protocol is up
Hardware is Tunnel
Internet address is 11.1.1.1/24
MTU 17846 bytes, BW 100 Kbit/sec, DLY 50000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.0.0.1
Tunnel MAC address 0000.5e00.5213
Tunnel Vlan-id 1
Tunnel protocol/transport Ethernet-GRE/IP Key 0x1, sequencing disabled Checksumming of packets disabled
Tunnel TTL 255
Tunnel transport MTU 1454 bytes
Tunnel transmit bandwidth 8000 (kbps) Tunnel receive bandwidth 8000 (kbps)
Last input 00:48:08, output never, output hang never
Last clearing of "show interface" counters 00:48:26
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 107
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1867 packets input, 161070 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
43 packets output, 4386 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out ind-uut#
--- 22:03:51 ---
44: 2013-01-30T22:03:51: %SCRIPT-6-INFO: {_haExecCmd: Executing cmd exec with ind-uut-a}


Device# show interface tunnel 2

Tunnel2 is up, line protocol is up
Hardware is Tunnel
Internet address is 10.1.1.1/24
MTU 1434 bytes, BW 100 Kbit/sec, DLY 50000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10::1
Tunnel MAC address 0000.5e00.5213
Tunnel Vlan-id 2
Tunnel protocol/transport Ethernet-GRE/IPv6
Key 0x2, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255
Path MTU Discovery, ager 10 mins, min MTU 1280
Tunnel transport MTU 1434 bytes
Tunnel transmit bandwidth 8000 (kbps) Tunnel receive bandwidth 8000 (kbps)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:48:28
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 106
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
```

Step 2 **show tunnel endpoints tunnel** *tunnel-interface*

This command displays tunnel interface endpoints and verifies if the tunnel is created correctly.

Example:

```
Device# show tunnel endpoints tunnel

Tunnel0 running in Ethernet-GRE/IP mode

Endpoint transport 10.1.1.1 Refcount 3 Base 0x2A98DD03C0 Create Time 3d02h
   overlay 10.1.1.1 Refcount 2 Parent 0x2A98DD03C0 Create Time 3d02h
 Endpoint transport 3.3.3.3 Refcount 3 Base 0x2A98DD0300 Create Time 3d02h
   overlay 10.1.1.3 Refcount 2 Parent 0x2A98DD0300 Create Time 3d02h
```

Step 3 **show tunnel mac-table tunnel** *tunnel-interface*

This command displays MAC table entries that are associated with a tunnel.

Example:

```
Device# show tunnel mac-table tunnel0
```

```
overlay-address 30.0.0.21, transport-address 192.168.0.50
mac-address 0000.1200.0001, vlan 400 Mac Age 3d06h

overlay-address 60.0.0.8, transport-address 120.0.40.2
mac-address 3010.e495.b058, vlan 10 Mac Age 00:01:00
```

Step 4 **show policy-map multipoint tunnel** *tunnel-interface*

This command displays the policy-map that is associated with a tunnel.

Example:

```
Device> show policy-map multipoint tunnel 1

Interface Tunnel 1 <--> 1.1.1.1
  Service-policy output: test
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      police:rate 300000 bps, burst 17898 bytes
      conformed 0 packets, 0 bytes;actions:transmit
      exceeded 0 packets, 0 bytes; actions:drop
        conformed 0000 bps, exceeded 0000 bps
```

Configuration Examples for QoS on Ethernet over GRE Tunnels

Example: QoS on Ethernet over GRE Tunnels

Configuring Ethernet over GRE (EoGRE) on the mobile node.

```
! configure the topology
mobile-node1(config-if)# interface GigabitEthernet0/1
mobile-node1(config-if)# ip address 10.21.1.1 255.255.255.0
mobile-node1(config-if)# no shutdown
mobile-node1(config-if)# exit
mobile-node1(config)# ip route 10.0.0.1 255.255.255.255 10.21.1.2

! Configure the interface used as the source of the tunnel
mobile-node1(config)# interface Loopback0
mobile-node1(config-if)# ip address 10.40.0.1 255.255.255.0
mobile-node1(config-if)# ipv6 address 2001:db8:2:40::1/64
mobile-node1(config-if)# no shutdown

! Configure the Ethernet over GRE IPv4 Tunnel
mobile-node1(config-if)# interface Tunnel1
mobile-node1(config-if)# mac-address 0000.0000.0001
mobile-node1(config-if)# ip dhcp client client-id ascii MN1@cisco.com
mobile-node1(config-if)# ip address dhcp
mobile-node1(config-if)# no ip redirects
mobile-node1(config-if)# no ip route-cache
mobile-node1(config-if)# tunnel source Loopback0
mobile-node1(config-if)# tunnel mode ethernet gre ipv4
mobile-node1(config-if)# tunnel key 1
mobile-node1(config-if)# tunnel vlan 10, 20
```

```
mobile-node1(config-if)# no shutdown
mobile-node1(config-if)# exit

Configuring Ethernet over GRE tunnel on the MAG

! Configure the topology
MAG(config)# interface FastEthernet1/1/5
MAG(config-if)# ip address 10.21.1.2 255.255.255.0
MAG(config-if)# ipv6 address 2001:db8:2:21::2/64
MAG(config-if)# no shutdown
MAG(config)# ip route 10.40.0.1 255.255.255.255 10.21.1.1

! Configure the interface used as source of the tunnel
MAG(config-if)# interface Loopback0
MAG(config-if)# ip address 10.0.0.1 255.255.255.0
MAG(config-if)# no shutdown

! configure the policy map
MAG(config)# policy-map tunnel-qos-policy
MAG(config-pmap)# class class-default
MAG(config-pmap-c)# police rate 200000 bps
MAG(config-pmap-c)# exit

! Configure the Ethernet over GRE IPv4 Tunnel
MAG(config)# interface Tunnel1
MAG(config-if)# ip address 10.11.1.1 255.255.255.0
MAG(config-if)# tunnel mode ethernet gre ipv4
MAG(config-if)# tunnel source Loopback0

! Configure a static GRE and VLAN ID for the tunnel
MAG(config-if)# tunnel key 1
MAG(config-if)# tunnel vlan 10, 20

!Associate the QoS policy to the tunnel interface
MAG(config-if)# tunnel endpoint service-policy output tunnel-qos-policy

! Enable ISG on the tunnel
MAG(config-if)# ip subscriber l2-connected
MAG(config-subscriber)# initiator unclassified mac-address
MAG(config-subscriber)# initiator dhcp
MAG(config-subscriber)# exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
iWAG commands	Cisco IOS Intelligent Wireless Access Gateway Command Reference

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for QoS on Ethernet over GRE Tunnels

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for QoS on Ethernet over GRE Tunnels

Feature Name	Releases	Feature Information
QoS on Ethernet over GRE Tunnels	Cisco IOS XE 3.13S	The QoS on Ethernet over GRE (EoGRE) Tunnels feature enables service providers to configure a common QoS policy for all endpoints. This feature supports dual high availability for a route processor. The following command was introduced by this feature: **tunnel endpoint service-policy output**.