# Troubleshoot IGP Flaps, Packet Loss, or Tunnel Bounce across a VPN Tunnel with EEM and IP SLAs

## Contents



## Introduction

This document describes what steps to take when you experience EIGRP/OSPF/BGP flaps over a DMVPN/GRE/sVTI/FlexVPN tunnel.

## Background Information

In order to troubleshoot this issue, the first question that needs to be answered is "Is this a VPN, routing protocol, or ISP issue?" In order to answer the question, connectivity tests across the underlay (usually the Internet or a private WAN) and overlay (usually the VPN tunnel) must be performed during the time of the flap/outage. Unfortunately these flap events can be transient and intermittent and as a result it can be difficult to perform these tests during the time of the issue. This document provides guidance about the use of the IP Service Level Agreement (SLA), track objects, and Embedded Event Manager (EEM) in order to collect this information at the time of the issue automatically.

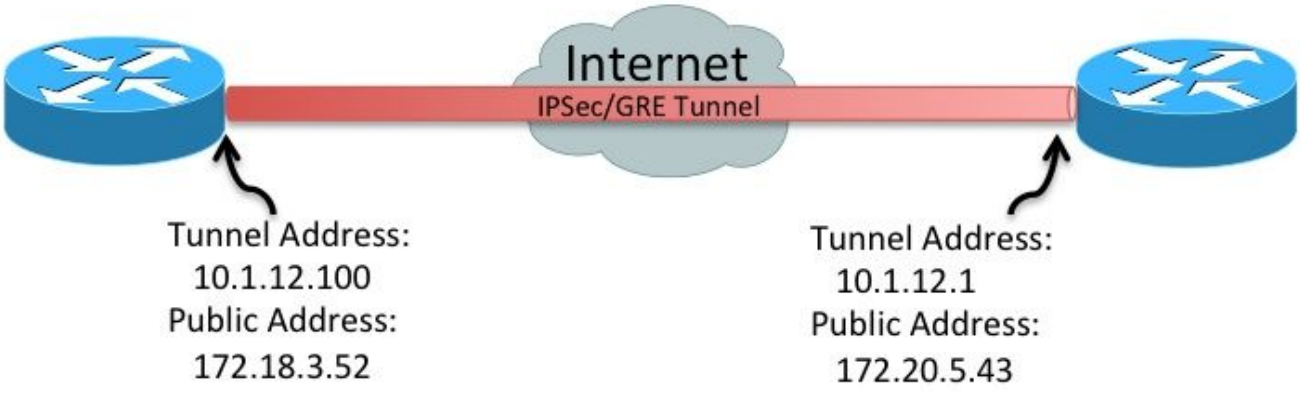
## Feature Information

IP SLAs are processes, that run on the router in the background, which test a number of network conditions. In this document, general IP connectivity is tested with the "icmp-echo" test.

A track object can then track the state of the IP SLA. Then, with an EEM applet, the state of the network can be recorded in the syslog buffer when the track object changes.

Utilize the network state recorded in the syslogs history to understand the state of the network during the flap/outage and determine whether there was a crypto, transport, or Interior Gateway Protocol (IGP) issue.

# Methodology




## Step 1. Define an SLA to track the underlay (Internet connectivity)

- Option A
  Public IP address to public IP address (172.18.3.52 > 172.20.5.43). Since the remote peer usually replies to ICMP this SLA only needs to be defined on one device.

```
ip sla 100
    icmp-echo 172.20.5.43 source-interface FastEthernet4
    frequency 5
ip sla schedule 100 life forever start-time now
```

- Option B **Note**: In some environments, Internet Control Message Protocol (ICMP) packets are blocked in the underlay/transport network. In these environments, udp-echo packets can be used instead of icmp-echo for IP SLA.
  IP SLA initiator (Left Router)

```
ip sla 100
 udp-echo 172.20.5.43 1501 source-ip 172.18.3.52 source-port 1501 control disable
 frequency 5
ip sla schedule 100 life forever start-time now
```

  IP SLA responder (Right Router)

```
ip sla responder
ip sla responder udp-echo ipaddress 172.20.5.43 port 1501
```

## Step 2. Define an SLA to track the overlay (Tunnel connectivity)

- Tunnel IP address to tunnel IP address (10.1.12.100 > 10.1.12.1)

```
ip sla 200
    icmp-echo 10.1.12.1 source-interface Tunnel100
    frequency 5
ip sla schedule 200 life forever start-time now
```

These SLAs send a single packet every five seconds to the defined peers. If the peer responds, the SLA is marked "OK". If it does not respond, it is marked "Timeout". The track objects monitor the

state of the SLA.

### Step 3. Define track objects to monitor the SLA states

- Underlay connectivity track object

```
track 100 ip sla 100
   delay down 15 up 15
```

- Overlay connectivity track object

```
track 200 ip sla 200
   delay down 15 up 15
```

When the track object changes, a message can be inserted in the syslogs.

### Step 4. Define an EEM applet to record when the track objects change

- Create an EEM applet for when the underlay transport fails and another for when it recovers

```
event manager applet ipsla100down
    event track 100 state down
    action 1.0 syslog msg "Underlay SLA probe failed!"
event manager applet ipsla100up
   event track 100 state up
   action 1.0 syslog msg "Underlay SLA probe came up!"
```

- Create an EEM applet for when the overlay transport fails and another for when it recovers

```
event manager applet ipsla200down
    event track 200 state down
    action 1.0 syslog msg "Overlay SLA probe failed!"
event manager applet ipsla200up
   event track 200 state up
   action 1.0 syslog msg "Overlay SLA probe came up!"
```

## Data Analysis

When an outage occurs, collect the output of the **show log** command. Look for the SLA messages shown in the previous section.

There are three potential scenarios:

1. Both SLAs fail. This means: Layer 3 connectivity across the underlay (Internet/MPLS) between the two peers was interrupted. This needs further investigation.There is no problem with the tunnel. It failed because it is a victim of the interruption of the underlay.
2. The Physical SLA does not fail, but the Tunnel SLA does. This means: Layer 3 connectivity across the Internet between the two peers works correctly.There is a problem with the tunnel. Further investigation of the tunnel is necessary.
3. Neither of the SLAs fail. This means: Layer 3 connectivity across the Internet between the two peers works correctly.Layer 3 unicast connectivity across the tunnel between the two peers works correctly.Layer 3 multicast connectivity across the tunnel is unknown. In order to test this, ping the multicast address used by the IGP.If the test works, then this indicates an application issue (EIGRP/OSFP/BGP). Further protocol investigation is necessary.