

Tracing process in IPv6 VPN Tunneling Networks

draft-peng-6man-tracing-option-04

Shuping Peng Huawei Technologies

Yisong Liu China Mobile

Ranxiao Zhao Huawei Technologies

Pingan Yang Huawei Technologies

Necessary information and mechanism are needed

- In order to construct a correct ICMPv4/v6 Time Exceeded Message at PE1 and send it to CE1, the following key information is required:
 - 1) **The IPv4/v6 address of the access interface at the P node**, which will be taken as the source address of the ICMPv4/v6 Time Exceeded Message.
 - If the P node does not have an IPv4 address, the IPv4 address of the PE1 will be taken as the source address of the ICMP(v4) message.
 - 2) **The VPN information**, which is used to identify the VPN, either using **the VPN ID or the Access Interface ID at the PE1**.
- However, currently this information is missing and an appropriate way is desired to collect and carry it to the right nodes.
- A **mechanism for** the router P to determine whether HL=0 is caused by a loop or a normal traceroute is also needed.

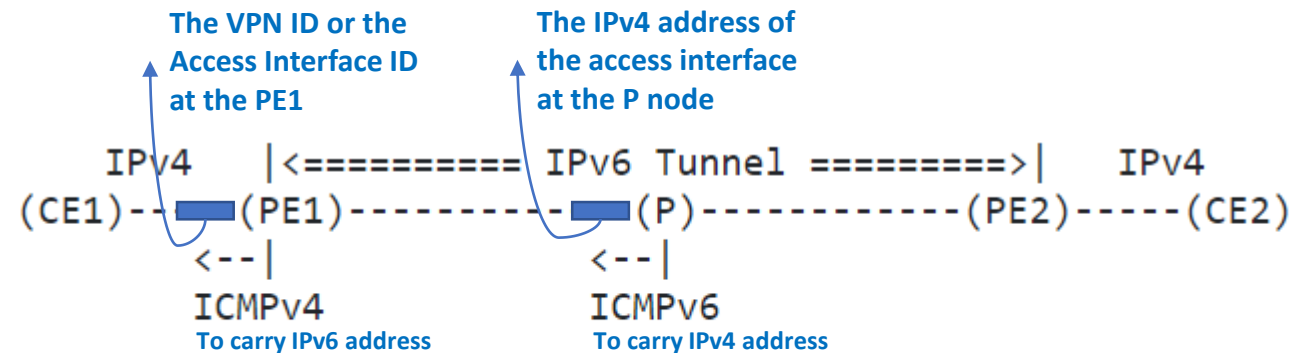


Figure 1. The tracing in IPv6 VPN tunneling networks

Updates since last IETF

- 4443 is referenced, but that's a MPLS tunneling document.
For IPv6 tunneling you might want to look at [RFC 2473](#).
- > RFC2473 is referenced, and the following text is added in the Introduction.
- “[RFC2473] defines the model and generic mechanisms for IPv6 encapsulation of Internet packets, such as IPv6 and IPv4.”

- Your comments are welcomed.
We would like to ask for working group adoption of this draft.