

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: April 24, 2014

Y. Yin
S. Jiang
G. Yan
Huawei Technologies Co., Ltd
October 21, 2013

IP Flow Path Trace Requirements
draft-yin-tsvwg-ipflow-pathtrace-ps-01

Abstract

This document describes the requirements of IP flow path trace. Network administrators need to get the real IP flow path information, of which a specific IP flow goes through heterogeneous network environments. It is also desired for more information relevant to the IP flow path. Based on the information, network administrators can locate possible faults of the network quickly or optimize network resource for better network performance.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 24, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

Internet-Draft

Flow Path Trace Requirements

October 2013

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Conventions Used in This Document	3
3.	Function Requirement for a new IP Flow Path Trace Mechanism .	4
3.1.	Requirement for path trace across heterogeneous network environments	4
3.2.	IP flow based path trace requirements	4
3.3.	Required information relevant to path	5
3.4.	Security requirements	6
4.	Security Considerations	6
5.	IANA Considerations	6
6.	Acknowledgements	6
7.	Informative References	6
	Authors' Addresses	7

[1.](#) Introduction

At present, the Internet Service Providers (ISPs) provides a wide variety of services, such as Internet access, lease line, mobile, Next Generation Network (NGN), Virtual Private Network (VPN), etc. Different service has different quality requirements and the ISPs make the Service Level Agreement (SLA) contracts with customers for each service. So when service failure or decline in the quality of service happens, the service provider's network administrator must locate reasons in the shortest time.

The current ISP networks may actually be constructed by heterogeneous network technologies, such as native IP, Multi-Protocol Label Switching (MPLS, [[RFC3031](#)]), Pseudo-Wire Emulation Edge to Edge (PWE3, [[RFC3985](#)]), Virtual Private Lan Service (VPLS, [[RFC4762](#)]), Layer 2 VPN (L2VPN, [[RFC4664](#)]), Layer 3 VPN (L3VPN, [[RFC4364](#)]), tunnels (such as IPinIP [[RFC1853](#)], Generic Packet Tunneling - GRE [[RFC2473](#)], etc.), translation, etc. The above mentioned IP services may be delivered across these heterogeneous network environments.

To locate the network fault quickly, IETF has defined the corresponding ping and trace functions for each network technology, independently. They are IP ping/trace using Internet Control Message

Protocol (ICMP) [[RFC0792](#)], LSP ping/trace [[RFC4379](#)], PW ping/trace, [[RFC5085](#)], [[RFC6073](#)], etc.

However, none of these technologies are able to gather the trace information of all these heterogeneous network environments.

Although trace packets, such as ICMP packets, can traverse these heterogeneous network environments, it does not record information regarding to these heterogeneous intermediate devices at all. Giving the fact, that many of current packets would transmit more than one network environments, it is still difficult trace the complete end-to-end paths.

Another issue of these ping/trace functions is path replicability. Most of these current ping/trace mechanisms are based on the triple of {source IP address, destination IP address, IP protocol number}. However, there are many Link Aggregation (LAG) or Equal-Cost Multi-Path (ECMP) scenarios in current networks; and many of network devices select forwarding interfaces based on the result of hash calculation on the quintuple {source IP address, destination IP address, source port number, destination port number, IP protocol number}. There are other load balancing algorithm, such as [[I-D.ietf-intarea-flow-label-balancing](#)][], which based on the triple of {source IP address, destination IP address, flow label} in IPv6. Therefore, the path traced by these ping/trace mechanisms may not be replicable by the IP flows at all. In other word, it is common that the real IP flows go through different paths from the result these ping/trace functions.

Furthermore, these current ping/trace mechanisms only provide very simple information of path, mainly the addresses of intermediate nodes only. It is far from sufficient information to determine the network fault and make dynamic adjustment based on it. More information, such as link bandwidth, link congestion, etc., is desired if a better path trace mechanism was going to be designed.

With the above mentioned issues of current ping/trace mechanisms, this document describes requirements for a new path trace mechanism. If all these requirements were met, network administrators should be able to easily get the real path information which a specific IP service flow goes through in the heterogeneous network environments, and also can get many more information regarding to intermediate

devices and links. Based on the information, network administrators can locate the possible faults of the network quickly and may optimize network resources better to provide better network performance for their customers. .

[2.](#) Conventions Used in This Document

Yin, et al.

Expires April 24, 2014

[Page 3]

Internet-Draft

Flow Path Trace Requirements

October 2013

L2VPN	Layer-2 Virtual Private Networks
L3VPN	Layer-3 Virtual Private Networks
VRF	Virtual Routing and Forwarding
LAG	Link Aggregation
ECMP	Equal-Cost Multi-Path

[3.](#) Function Requirement for a new IP Flow Path Trace Mechanism

[3.1.](#) Requirement for path trace across heterogeneous network environments

A new IP flow path trace mechanism should be able to traverse heterogeneous network environments and gather the path information of intermediate devices and links. The heterogeneous network environments include native IPv4, native IPv6, MPLS, PWE3, VPLS, L2VPN, L3VPN, tunnels, translation, etc.

The new IP flow path trace mechanism should trace an end-to-end path or paths, no matter what intermediate network environment may go through. It should gather the information, described in [Section 3.3](#), and return them to the initiating node, which is normally the source of the end-to-end path.

The trace function may be trigger by a remote network manage device through a management protocol and the trace result may be automatically report back to this remote network manage device. However, it is independent from the requirements of the IP flow path trace mechanism.

[3.2.](#) IP flow based path trace requirements

Many IP services are managed based on IP flow. Between two giving nodes, there may be more than one IP flows and each IP flow may take different path, because the triple {source IP address, destination IP address, IP protocol number} are not sufficient to decide the path.

One of the purposes of the required new IP flow path trace mechanism is to trace the real path, which a specific IP service goes through. This would enable the network administrator to manage the network resource on this specific path in order to provide the best performance.

Therefore, the new required path trace requirements should be IP flow based. With a giving IP flow information, which is identified by the quintuple {source IP address, destination IP address, source port number, destination port number, IP protocol number} or triple {source IP address, destination IP address, flow label} in IPv6, the

new IP flow path trace mechanism should trace its end-to-end path or all possible paths.

[3.3.](#) Required information relevant to path

This section describes the information is desired when a new IP flow path trace mechanism is designed.

- o Intermediate node information: the identification information of each node which the specific IP flow goes through in the network. The information may be IP address, Router ID or MPLS LSR ID of each node.
- o Incoming interface and outgoing interface information: the incoming interface information and outgoing interface information of each node which the specific IP flow goes through in the network. The information must include the interface's IP address and may include interface name information.
- o MPLS label information: the MPLS forwarding label information if the flow goes through MPLS network. The information should include the incoming label and the outgoing label information of

the LSP. If VRF or PW are used to bear the IP flow, the information should include the incoming label and the outgoing label information for the VRF and PW.

- o Link bandwidth information: the link bandwidth information of the incoming interface and outgoing interface of each node which the IP flow goes through in the network. The information should include the total bandwidth and the current bandwidth usage ratio.
- o Link congestion information: the link congestion information of the incoming interface and outgoing interface of each node which the IP flow goes through in the network. The information should include the indication of congestion or not, further, usage information of the Quality of Service (QoS) queue which IP flow belongs to.
- o LAG&ECMP information: if outgoing interface is LAG or exist ECMP, the system must be able to accurately determine the load balance forwarding choice of the real IP, and also should get the LAG or ECMP number information.
- o Tunnel information: the information whether the IP Flow is tunneled and the information regarding to the tunnel. It may include the intermediate devices the tunnel transmits over.

- o Translation information: the information how the IP flow has been translated by a translation intermediate devices. It should include the mapping information from original address and port to translated address and port.
- o More information: more path trace information may be extended in the future so that more information relevant to IP flow path can be gathered.

3.4. Security requirements

- o Anti-DDOS (Distributed Denial of Service)
An attacker can launch a number of tracing processes to the network nodes, resulting in DDOS attacks. So the network node should implement flow control for the messages of the new tracing

function to avoid the attack.

- o Prevention of Network Information Spying Attack
The tracing function may enable an attacker to collect the information of the network, including topology, bandwidth, usage rate, etc. There must mechanisms to prevent such a threat and system information leak.

[4.](#) Security Considerations

The [Section 3.4](#) presents the security consideration/requirements for a solution that design to meet the IP flow path trace requirements.

[5.](#) IANA Considerations

This draft does not request any IANA action.

[6.](#) Acknowledgements

The authors wish to acknowledge the important contributions of Zhenbin Li and Mach Chen.

This document was produced using the xml2rfc tool [[RFC2629](#)].

[7.](#) Informative References

- [I-D.ietf-intarea-flow-label-balancing]
Carpenter, B., Jiang, S., and W. Tarreau, "Using the IPv6 Flow Label for Server Load Balancing", [draft-ietf-intarea-flow-label-balancing-02](#) (work in progress), October 2013.
- [RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, [RFC 792](#), September 1981.

- [RFC1853] Simpson, W., "IP in IP Tunneling", [RFC 1853](#), October 1995.
- [RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", [RFC 2473](#), December 1998.
- [RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", [RFC 2629](#), June 1999.

- [RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", [RFC 3031](#), January 2001.
- [RFC3985] Bryant, S. and P. Pate, "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", [RFC 3985](#), March 2005.
- [RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", [RFC 4364](#), February 2006.
- [RFC4379] Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures", [RFC 4379](#), February 2006.
- [RFC4664] Andersson, L. and E. Rosen, "Framework for Layer 2 Virtual Private Networks (L2VPNs)", [RFC 4664](#), September 2006.
- [RFC4762] Lasserre, M. and V. Kompella, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling", [RFC 4762](#), January 2007.
- [RFC5085] Nadeau, T. and C. Pignataro, "Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires", [RFC 5085](#), December 2007.
- [RFC6073] Martini, L., Metz, C., Nadeau, T., Bocci, M., and M. Aissaoui, "Segmented Pseudowire", [RFC 6073](#), January 2011.

Authors' Addresses

Yuanbin Yin
Huawei Technologies Co., Ltd
Q15, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: yinyuanbin@huawei.com

Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: jiangsheng@huawei.com

Gang Yan
Huawei Technologies Co., Ltd
Q15, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: yangang@huawei.com