INTERNET-DRAFT
Expiration Date: January 2002

Satoru Matsushima
Japan Telecom
Ken-ichi Nagami
Toshiba Corp
Hideo Ishii
Asia GlobalCrossing
Yuichi Ikejiri
NTT Communications
July 2001

TTL Processing expansion for 1-hop LSP
<draft-satoru-mpls-1hop-lsp-01.txt>

Status of this Memo

Abstract

The structure that LSP was handled as 1-hop became necessary. It came from the requirement of LSP topology management in the MPLS network. As for VPN services using LSP, VPN customers may be confused by receiving ICMP packet, e.g., traceroute includes the routers in the MPLS backbone un-belonging to the user's VPN topology view, from non VPN topology. And ISP may not want to users know the network topology because of ISP may want to change the LSP route due to traffic

engineering purpose. However, according to [MPLS-ARCH] and [MPLS-SHIM] does not include such behavior. So, we propose to specify the specification to provide "1-hop LSP" that is the way of 1 TTL decrement method onto a LSP at an egress LSR. And we also discusses LSP's keepalive method using the 1-hop LSP.

---

1. Overview

It is very useful to show 1-hop LSP for IPv4 packet in some situations. However, according to [MPLS-ARCH] and [MPLS-SHIM]. basically, LSP can not be shown to 1-hop for IP packet, because of the IPv4 TTL is decreased by the amount of hops within the MPLS domain. This document specifies the way to realize 1-hop LSP which is done by expanded TTL processing of LSRs.

The 1-hop LSP can be useful in the following situations:

- If VPN service was provided onto MPLS domain, then the VPN providers can hide their backbone network topology from VPN customers.

- LSP was treated as 1-hop path, then LSP can be tunnel deviced.

- LSP's keepalive can be possible by enabling 1-hop LSP at the LSR.

To enable 1-hop LSP, the TTL processing is necessary for only in ingress and egress LER. However, to do the "Keep-Alive" of the LSP, the same level of expansion is required for egress LER on core LSRs.

2. Definition of 1-hop LSP

The following figure shown an example of 1-hop LSP. There is a 1-hop LSP between an ingress LSR (LERi) and egress LSR (LERe). In the 1-hop LSP, a value of MPLS TTL is decreased at subsequence LSRs. On the other hand, a value of IP TTL is set to one less than the incoming TTL value at the LERe. The LERe does not set the IP TTL value from MPLS TTL value. In this situation, a customer can realizes the MPLS network topology as Ra -> LERi -> LERe -> Rb. It means that customer does not realize intermediate routers on the 1-hop LSP.

```
          Ra -> LERi -> LSR -> LSR -> LERe -> Rb -> Destination
                 |<---- 1-hop LSP ---->|                host/network
IP TTL    10      9      9      9       8     7
MPLS TTL          9      8
```

In other words, LSP which copes with FEC which corresponds to Destination Address is operated with MPLS Domain as 1-hop LSP.

3. Models and methods of 1-hop LSP

A TTL Processing expansion is given to an ingress LER and an egress LER for 1-hop LSP. We have following three cases.

(a) Basic process of 1-hop LSP

When an IP packet is first labeled in ingress LER, the TTL field of the label stack entry is set to have the value which could reach an egress LER fully. The MPLS-TTL is usually set to have the value of 255 in most cases. (The procedure of IP-TTL decrementation is assume to be finished before the event of MPLS labelling in the ingress LER.)

The egress LER pops a label and sets IP TTL value to one less than that of the received IP packet. The egress LER does not replace the value of IP TTL with the incomming MPLS TTL. As a result, the value of IP TTL of the incomming packet at the ingress LER is one less than that of the outgoing packet at the egress LER.

(b) 1-hop LSP with hierarchical labels

When the LSP with depth m label is set to 1-hop LSP, the LSP provides 1-hop LSP process to depth m-1 LSP. The TTL process is almost the same as the case of (a) except that an IP packet is replaced by a depth m-1 labeled packet.

Example:

```
                   Ra -> LERi -> LSR -> LSR -> LSR(e) -> LSR -> Destination
                           |<--- 1-hop LSP ---->|                host/network
IP TTL             10      9      9      9      9         9
MPLS TTL                   255    255    255    254       253    (depth 1)
MPLS TTL(1-hop LSP)        255    254    253    popped           (depth 2)
```

(c) 1-hop LSP with Penultimate Hop Pop (PHP)

When a label stack may be popped at the penultimate LSR of the 1-hop LSP, rather than at the LER, the TTL of the exposed label or IP is not updated. The process at the egress LER is the same as the case of (a) and (b).

Example:

```
          Ra -> LERi -> LSR -> LSR -> LERe -> Rb -> Destination
                    |<-- 1-hop LSP ->|                    host/network
IP TTL    10      9      9      9       8     7
MPLS TTL          255    254    popped
```

This is a fundamental mechanism for making 1-hop LSP, and the model which forms 1-hop LSP is divided by the label distribution method; DU or DoD.

In this document, The model which realizes 1-hop with DU is defined as "Cloud model", and the model which realizes 1-hop with DoD is defined as "Per LSP model". These are explained in the following.

3.1 Cloud model

In order to use 1-hop LSP on DU, we must decide whether the whole MPLS Cloud shoud be used for 1-hop, or used as just an ordinary LSP. This is because, when the LSP set-up is being done on the DU, each LSR on the LSP cannot be informed of the characteristics of the LSP from the ingress LSR.

This kind of method is not realistic however. Instead, it will work mostly well as 1-hop LSP if "out-going TTL" is defined on BCP such that the smaller value of TTL is chosen as the "out-going TTL" by comparing the MPLS TTL and the IP TTL on the egress LER where the Label is "popped".

However, in case of the value of the IP TTL being larger than the value of MPLS TTL when the Label is "popped", it will not work as 1-hop LSP.

3.2 Per LSP model

When LSP set-up is being done on the DoD, each LSR on the LSP can be informed of the characteristics of the LSP from the ingress LSR. In this case, if the expansion attribute that defines TTL processing method is installed, then we can choose between the choice of LSP types; one is 1-hop LSP per each LSP, and the other is the ordinary LSP. The Orderd Distribution will be needed as well. This is because if the ingress LER is not informed by the egress LER of its LER's choice of LSP type, there is no way for ingress LER to know if it should do the TTL processing on a packet for 1-hop LSP or not.

The TTL processing method is completely independent of the TTL processing methods in other LSPs in Per LSP model due to the open choice of TTL processing methods is available in each LSP. (When the "LSP merge" which is done with ATM-LSR is made, Per LSP model is not applied even if it is DoD.)

Therefore, basically the Cloud model and the Per LSP model can coexist.

4. Applicable Areas of "1-hop LSP"

This section explains the desirable packets and traffics carried by "1-hop LSP", and the types of undesirable packet and traffic carried by "1-hop LSP".

(a) The case where 1-hop LSP shall be applied

- LSP KeepAlive (See section 5).
- The case where LSP is layered with "1-hop LSP" exists on its higher layer.

(b) The case where "1-hop LSP" is desirably applied

- IP-VPN packets, such as [MPLS-VPN].
  (It would be applied by motivation that is described in Section 1. But some Layer2-VPN is excluded from this case.)

(c) The case where "1-hop LSP" shall not be applied

- The packets that test the carry-way of LSP

(i.e. "ping" and "traceroute" used by operators)
If those packets was carried by "1-hop LSP", the purpose that test the carry-way of LSP can not be achieved.

These mean we may not differentiate whether it is "1-hop LSP" or not, just by looking at the unit of LSP. This is because if the aim is different, LSP may have to be "1-hop" or may not have to be "1-hop", even if the packets are carried through the same LSP. This causes the LSR must decide whether packets and traffics should be activated as "1-hop LSP" or not, by their aims. Incidentally, the setting of LSP activation status should be able to be changed for operators desired use.

5. The Possible to LSP "KeepAlive" using 1-hop LSP

5.1 Background

This "LSP KeepAlive" ability is extremely important for the applications which use LSP but cannot know the state of LSP itself (for instance, consider the situation where BGP/MPLS VPNs [MPLS-VPN] are used; they will recognise the network as "available" only if the possibility of the IP accessibility to the PE exits, whatever the state of the LSP).

5.2 Method of "LSP KeepAlive" process

The "KeepAlive" of LSP is possible by the use of IP Packet transmission to FEC from the ingress LER with the minimum IP TTL (minimum value=1) through 1-hop LSP. This is because if there is a cut within LSP then there will be no reply.

In order to carry out "KeepAlive" of LSP, the expansion process is also require for the core LSR such that IP TTL will not be replaced by MPLS TTL, just like in the egress LER. This is because, if there is a cut within LSP the core LSR will "pop" the label. This means that the original core LSR will be made to act as an egress LER.

The reply can be expected from the entire installed, if, such as ICMP ECHO is used for setting of the IP Packet in this situation.

The TTL does not have to, or more precisely, should not have a value of 1 for reply. In case of TTL value on the reply message being 1, it will go to the opposite side of LSP "KeepAlive" since the LSP is a one-way path. This LSP "KeepAlive" cannot be "KeepAlive" for each

LSP.

The TTL value on the LSP KeepAlive's reply message should have large enough value. Also, if there is no route for the reply message to return, it will look as though the healthy LSP does not exit.

6. Concern

In The case that the outgoing TTL of a labeled packet is set to the maximum value 255 at an ingress LER, it is difficult to detect loops in the MPLS cloud, because the value of the IP TTL field is not replaced with the outgoing TTL value when a label is popped or the resulting label stack is empty.

7. Security Considerations

This document does not introduce new security issues other than those present in the [MPLS-SHIM] and may use the same mechanisms proposed for this technology.

8. Acknowledgments

Thanks to Ikuo Nakagawa, Hiroshi Esaki and JANOG(Japan Network Operators' Group) people for their comments.

9. References

[MPLS-ARCH] Rosen, E., Viswanathan, A. and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[MPLS-SHIM] Rosen, E., Rekhter, Y., Tappan, D., Fedorkow, G., Farinacci, D. and A. Conta, "MPLS Label Stack Encoding", RFC 3032, January 2001.

[MPLS-VPN] Rosen, E., et. al., "BGP/MPLS VPNs", draft-rosen-rfc2547bis-03.txt, March 2001.

10. Authors' Address:

Satoru Matsushima
Japan Telecom
4-7-1, Hatchobori, Chuo-ku
Tokyo, 104-8508 Japan
Phone: +81-3-5540-8214
Email: satoru@japan-telecom.co.jp

Ken-ichi Nagami
Communication Platform Laboratory, R&D Center, Toshiba Corporation
1, Komukai Toshiba-cho, Saiwai-ku
Kawasaki, 212-8582, Japan
Phone: +81-44-549-2230
EMail: ken.nagami@toshiba.co.jp

Hideo Ishii
Asia GlobalCrossing
4-3-20, Toranomon, Minato-ku
Tokyo 106-0001 Japan
Phone: +81-3-5408-1716
Email: hishii@gblx.net

Yuichi Ikejiri
NTT Communications Corporation
1-1-6, Uchisaiwai-cho, Chiyoda-ku
Tokyo 100-8019 Japan
Phone: +81-3-6700-8540
Email: ikejiri@ntt.ocn.ne.jp