

TRILL working Group
Internet Draft
Intended status: Standards Track

Rohit Watve
Tissa Senevirathne
Chandan Mishra
CISCO
Gayatri Ramachandran
ARISTA Networks
September 17, 2013

Expires: March 2014

**Pro-active connectivity monitoring for TRILL
draft-rohit-trill-proactive-oam-03.txt**

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

This Internet-Draft will expire on July 18, 2009.

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 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.

Abstract

Pro-active fault monitoring for TRILL monitors all the paths between any two given RBridges in the network. Number of paths to be monitored can be of exponential order based on the distance between two RBridges. In this document novel fault monitoring mechanism based on a distributed approach is presented.

Table of Contents

| | |
|---|--------------------|
| 1. Introduction..... | 2 |
| 2. Conventions used in this document..... | 3 |
| 3. Motivation..... | 3 |
| 4. Solution overview..... | 6 |
| 4.1. Details for monitoring paths upto 2nd hop Rbridge..... | 8 |
| 5. Frame formats..... | 9 |
| 5.1.1. Pro-active fault monitoring request..... | 9 |
| 5.1.2. Pro-active Payload discovery request..... | 10 |
| 5.1.3. Pro-active Payload discovery response..... | 12 |
| 5.1.4. Pro-active fault notification..... | 13 |
| 6. Formal Syntax..... | 16 |
| 7. Security Considerations..... | 16 |
| 8. IANA Considerations..... | 16 |
| 9. Conclusions..... | 16 |
| 10. References..... | 16 |
| 10.1. Normative References..... | 17 |
| 10.2. Informative References..... | 17 |
| 11. Acknowledgments..... | 17 |
| Appendix A. Sample report..... | 19 |
| A.1. Summary Report per monitor..... | 19 |
| A.2. Detail Report..... | 19 |
| A.2.1. <H2>..... | 20 |
| A.2.1.1. <H3>..... | 20 |
| A.2.1.1.1. <H4>..... | 20 |
| A.2.1.1.1.1. <H5>..... | 20 |
| A.3. C type usage is messages..... | 20 |

1. Introduction

Pro-active fault monitoring is necessary for all OAM solutions. It gives network service providers confidence about the health of their

<Lastname>

Expires March 17, 2014

[Page 2]

network. Whenever network service is provided to customers with SLA (Service Level Agreement), it becomes even more important to monitor the network pro-actively. In traditional Layer-2 networks (CE) pro-active fault monitoring is done based on VLANs. Since spanning-tree ensures that there is a single path between any two nodes, it is straightforward mechanism to monitor path between 2 given RBridges and given VLAN.

TRILL Base Protocol Specification [[RFC6325](#)] provides a method for forwarding Layer 2 data frames over multiple active links. There can be number of ECMPs (Equal Cost Multiple Paths) between any two given TRILL RBridges. As the number of hops between given two RBridges increases, number of ECMPs increases exponentially. Pro-active monitoring in this case needs to monitor all the ECMPs between two given RBridges.

TRILL OAM draft [[TRILLOAM](#)] proposes OAM suite for TRILL. This draft is for adding pro-active functionality to the OAM suite. It extends C-types defined in TRILL OAM draft, for pro-active monitoring.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC-2119](#) [[RFC2119](#)].

3. Motivation

As we discussed in the introduction, number of paths to be tested increases exponentially as the number of hops between ingress and egress RBridge increases. Identifying the header parameters (mac/IP/L4 addresses) to exercise each unique path is a hard problem and needs information about hashing functions from each intermediate RBridge.

Sending test packets, with random header parameters, expecting that will exercise different ECMPs is one option. But in this case number of packets that need to be sent can be even higher than total number of ECMPs.

In this document we take a different approach to address this problem.

Testing end-to-end connectivity means, testing connectivity of all links along the path as well as exercising switching on all intermediate RBridges. Instead of doing it end to end, same can be done after splitting it into multiple short paths, such that, paths

<Lastname>

Expires March 17, 2014

[Page 3]

overlap to cover complete end-to-end connectivity. If each such short path is limited only to two hops, it brings down number of packets to be sent from exponential order of number of hops (k^n) to order of $(k^3)*n$, where k is assumed to be number of ECMPs for each hop for simplification of calculation and n is number of hops between the Ingress and Egress Rbridges.

Consider following Figure 1. In the figure, Rbridges are numbered from 1 to 10. The problem is to monitor end-to-end connectivity between Rbridge 1 and 10.

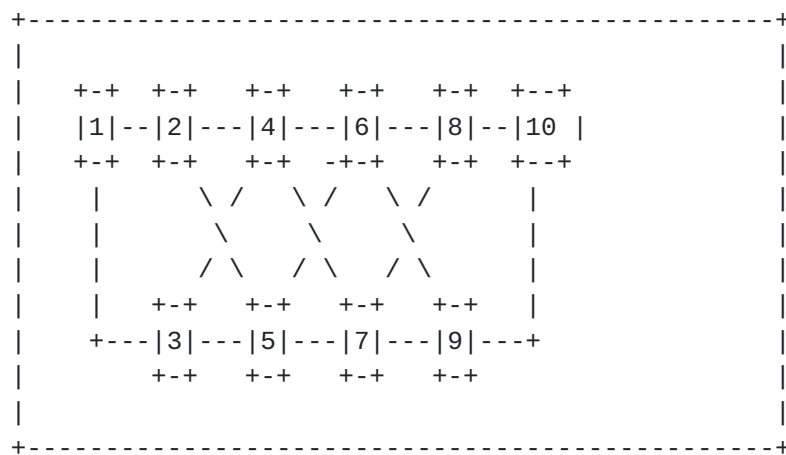


Figure 1 Example network.

In above Figure 1, Rbridges 2 and 3 are connected to Rbridges 4 and 5, Rbridges 4 and 5 are connected to Rbridges 6 and 7. Rbridges 6 and 7 are connected to Rbridges 8 and 9.

Total number of ECMPs between RBridge 1 and RBridge 10 is -
 $2 \times 2 \times 2 \times 2 = 32$

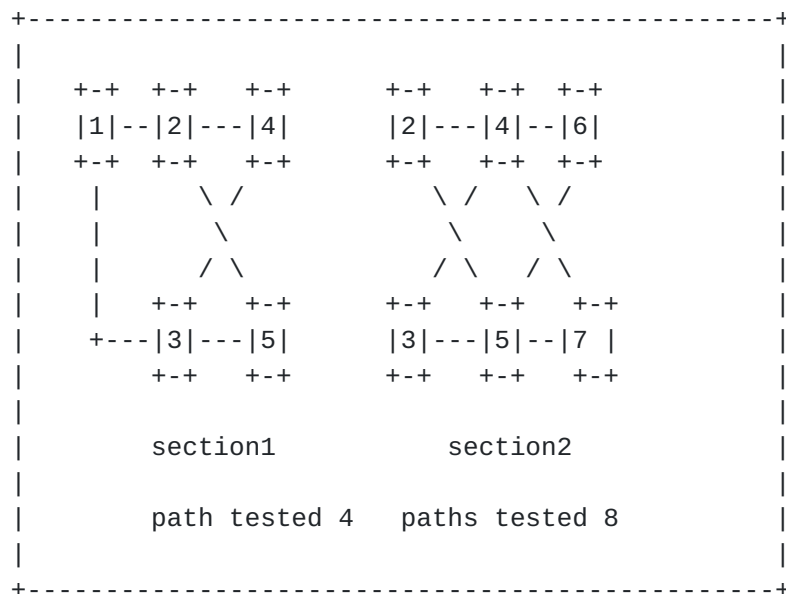
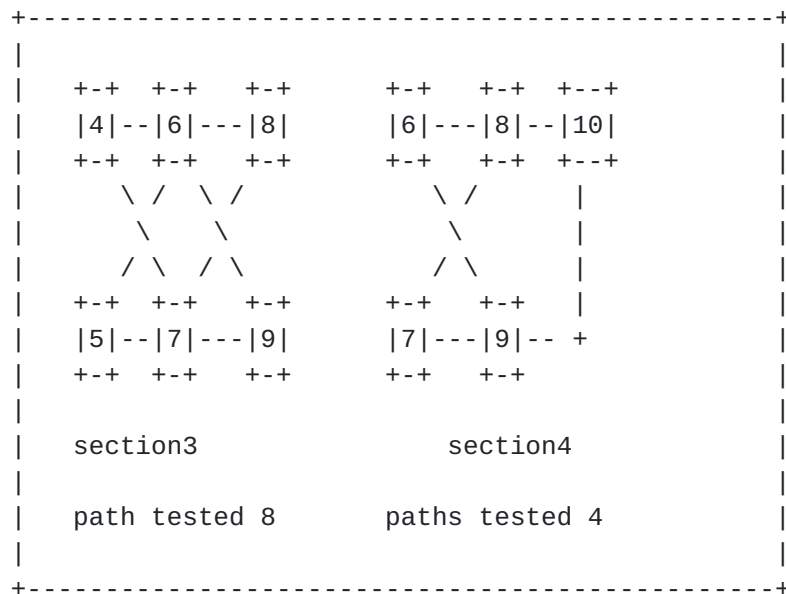
Hence Rbridge 1 will need to send 32 packets to test all ECMPs to Rbridge 10, assuming Rbridge 1 knows payloads required to exercise all these paths.

Above network can be split into four overlapping sections as shown in Figure 2 and Figure 3. If we test all paths between Ingress and Egress Rbridges of each section then all paths between 1 and 10 will be tested.

<Lastname>

Expires March 17, 2014

[Page 4]

Figure 2 [Section 1](#) and 2 for network in Fig.1Figure 3 [Section 3](#) and 4 for network in Fig.1

In Figure 2, for the [section 1](#), the number of paths between RBridges 1 and 4 is 2 and number of paths between RBridges 1 and 5 is 2. Hence total number of paths to be tested for sub-network1 is 4.

<Lastname>

Expires March 17, 2014

[Page 5]

Similarly, number of paths between RBridges 2 and 6 is 2, between RBridges 2 and 7 is 2. Number of paths between RBridges 3 and 6 is 2 and between RBridges 3 and 7 is 2.

Hence total number of paths to be tested is 8.

Similarly from Figure 3. total number paths to be tested for section3 is 8 and for [section 4](#) is 4.

Note that, in the above example network, maximum number of paths to be tested by any given Rbridge is limited to 8. Hence load of monitoring network is now distributed. Also total number of paths tested is $4+8+8+4=24$.

Note that if Rbridge 1 was to do testing for all paths, number of paths to be tested would be 32. As the complexity of the network increases and number of paths between Ingress and Egress Rbridges increases, the mechanism proposed here will yield even more benefits.

4. Solution overview

Here we present high level overview of the solution. More details are discussed in the subsequent sections.

Pro-active fault monitoring is initiated by the user. As part of the request, user identifies a VLAN and 2 RBridges - Ingress and Egress RBridges. All Equal Cost Paths ECMPs on this vlan and between these two RBridges need to be monitored. User provides total time interval for monitoring session as the part of the request.

Here are the high-level steps of the mechanism

1. Ingress Rbridge starts connectivity tests for paths upto its 2nd hop Rbridge(s)(on the path to egress RBridge).
2. If 2nd hop Rbridge is egress Rbridge, it stops the test.
3. Else it requests its 1st hop Rbridge(s) (on the path to egress), to initiate the tests, starting with step1.

Once the request is distributed, whenever a fault is detected, it is indicated to the Originator Rbridge using a fault notification message which includes fault details.

Consider Figure 4 as example network. Let us assume user requests proactive fault monitoring between ingress RBridge RB1 and egress

<Lastname>

Expires March 17, 2014

[Page 6]

RBridge RB5. P1 to P5 are the Egress ports along the ECMPs between RB1 and RB5.

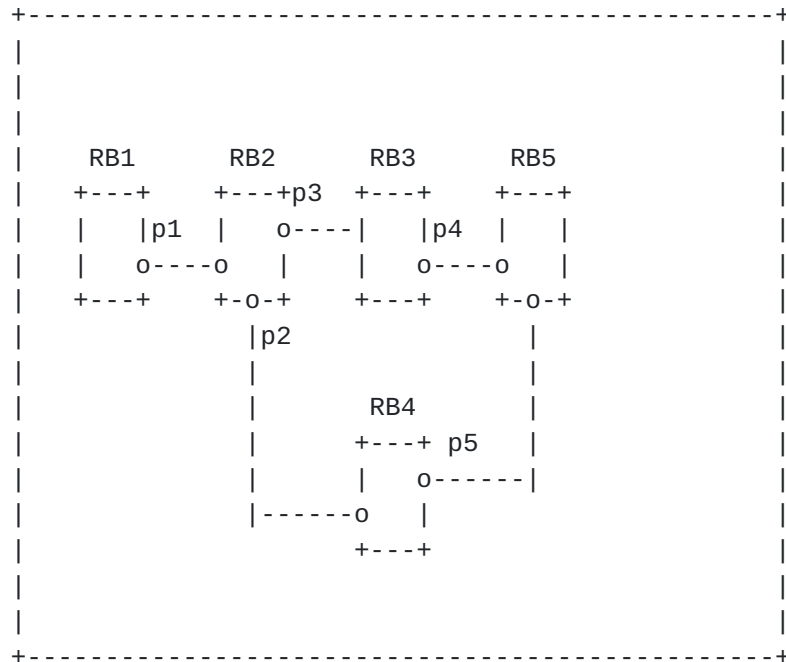


Figure 4 Example network.

As per step1, RB1 tests all paths upto its 2nd hop Rbridge on the path along RB5.

For that, RB1 sends 'payload request' message to its 1st hop Rbridges on the path along RB5. RB1 looks up its local forwarding table, and finds that p1 is Egress port for path towards RB5. It then sends 'payload request' with TTL=1 on p1. RB2, will reply back with 2 payloads say PL1 and PL2, for taking path along ports p3 and p2, respectively.

RB1 now sends two packets with payloads PL1 and PL2, and TTL=2. When RB1 receives 'hop count expiry' message for both, it confirms that paths up to its 2nd hop Rbridge(s) are fault-free(i.e. paths between RB1 and RB3 , as well as between RB1 and RB4 are fault-free).

As per step3, RB1 also forwards the 'pro-active fault monitoring request' message defined in [section 5.1.1](#), to monitor connectivity, to its 1st hop Rbridges along the path. It does so by sending request with TTL=1, on port p1.

<Lastname>

Expires March 17, 2014

[Page 7]

RB2 on receiving this request, will repeat the step1. It will send 'payload request' with TTL=1, on port p2 and p3. For each request, it will get one payload, say PL3 for request sent on p2 and PL4 for request sent on p2. It will test paths upto its 2nd hop Rbridges, by sending a packet with payload PL3 on port p2 and a packet with payload PL4 on port p3 and TTL=2.

As RB2 will receive 'hop count expiry' message from RB5, it will not forward the requests for monitoring paths till RB5, to its 1st hop Rbridges.

4.1. Details for monitoring paths upto 2nd hop Rbridge

For a given egress TRILL RBridge, local TRILL routing table can provide information about different next hop Rbridges/Egress ports to exercise the ECMPs.

We propose to send 'Payload Discovery request' message on each of these ports, with TTL=1. 'Payload Discovery request' ([section 5.1.1.](#)) message carries information about egress TRILL RBridge (RB5) in the original request made by the user.

Based on the egress RBridge (RB5), each 1st hop Rbridge looks up its TRILL forwarding tables, and for each equal cost multi path towards egress RBridge (RB5) identifies a unique inner destination MAC addresses, that will exercise the ECMPs towards egress Rbridge-id. These MAC addresses will be sent back in a 'Payload Discovery response packet'.

The source mac address is not used for payload generation, as it might be learnt by other Rbridge, if the packets are originated by TRILL Edge Rbridges. Well known source mac address is used, so that it will not be used by any real data packets. Ethtype is fixed to TRILL OAM Diagnostic ethtype to restrict these frames from leaving TRILL network (refer [section 6.2](#), from [\[TRILLOAM\]](#)). VLAN is specified by the user as a part of the request. For payload generation, nickname of the requester Rbridge, provided in 'payload generation request'([section 5.1.2](#)), is used as ingress Rbridge nickname. Egress Rbridge nickname provided in the request is used as Egress Rbridge nickname for payload generation.

The current TRILL RBridge, receives list of destination mac addresses on each port on ECMP. It constructs 'loopback message' (TRILLOAM) message with TTL=2 and these mac addresses as inner destination mac addresses and sends these on ports on which corresponding mac address was received.

Each packet sent, will now test the switching at next hop and test all links on the path taken by the packet. The inband or out of band ICMP 'hop count expiry response' (TRILLOAM), will confirm that both are fault-free. When all such responses are received, it will confirm that all paths towards egress Rbridge are error free, till 2nd hop. If there is a fault, fault details are sent to the originator Rbridge. If current Rbridge itself is the originator Rbridge, it saves the fault information.

Payload generation request is sent periodically based on the 'Payload generation request time interval' specified in the user request. Test packets are also sent at an 'test time interval' provided by the user. Finally this whole monitoring process is continued till the 'Monitor time interval', also specified by the user. 'Pro-active fault monitoring request' defined in next section is used for forwarding the request to 1st hop Rbridges.

5. Frame formats

5.1.1. Pro-active fault monitoring request

Pro-active fault monitoring request includes C-type 44 which provides Egress Rbridge ID and originator Rbridge ID. It also provides information about timers required in fault monitoring. C-type 4 (interested vlan) is included in the request to indicate monitored vlan, if the request packet is not using the same vlan. Source Mac address and ethtype are fixed to the values used in the request packet. Pro active fault monitoring message is represented by TRILL OAM message code 26.

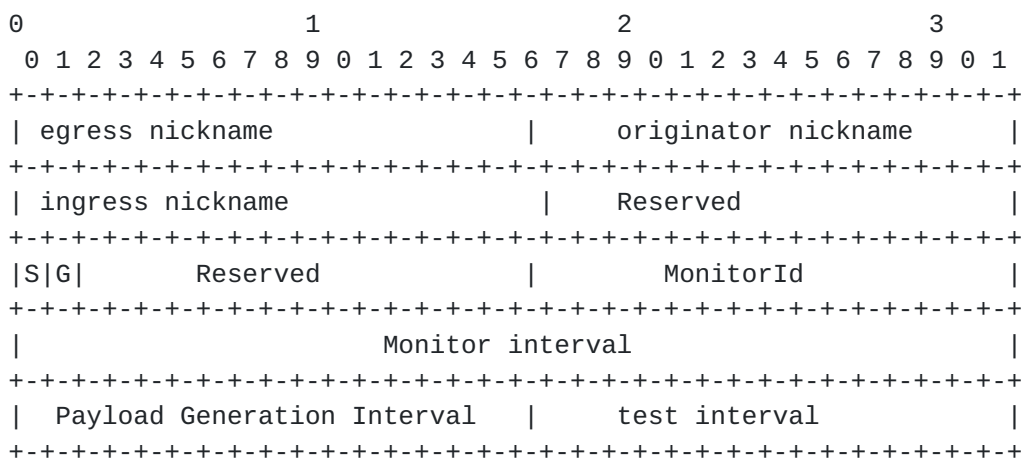


Figure 5 Pro-active fault monitoring request details (C-type 44)

<Lastname>

Expires March 17, 2014

[Page 9]

Egress nickname (2 octets): nickname of the Egress/egress Rbridge.

Originator nickname (2 octets): nickname of the originator Rbridge.

Ingress nickname (2 octets): nickname of the ingress Rbridge.

S (1 bit), start/stop request: if set to 1, specifies request to start monitoring, if set to 0, specifies request to stop monitoring.

G (1bit); Global stop, when set to 1, stops all pro-active monitoring requests on this Rbridge requested by same Originator RBridge, irrespective of other information in the C-type. Set to 1 only for debugging.

Reserved (14 bits):

MonitorId (16bits): Identifier for the current session. It is generated by Originator Rbridge such that it is unique locally, and propagated while forwarding request to next hops. MonitorId, combined with Originator Rbridge ID, forms unique identifier for fault monitoring session.

Monitor interval (4octets): total interval of fault monitoring session in seconds. 0 is a special value, indicating it needs to run till request to stop comes.

Payload Generation Interval(2 octets): interval for refreshing payload parameters by sending payload generation request in seconds.

Test interval (2 octets): interval for sending test packets with TTL=2, for testing paths till 2nd hop in seconds.

5.1.2. Pro-active Payload discovery request

C-type 'Payload discovery request for pro-active monitoring' is different from Payload Discovery request defined in section 8.2 in [\[TRILLOAM\]](#). This C-type by definition allows use of any Destination Mac address for payload generation. It also expects that response will include payloads for exercising all available ECMPs. Along with this new type, interested vlan (ctype 4) is also specified, if packet is not using same vlan. Source Mac address and ethtype are fixed to the values used in the request packet. Payload discovery message is represented by TRILL OAM message code (22).


```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| egress nickname                |   originator nickname        |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| ingress nickname                |   Requester nickname        |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Figure 6 Pro-active Payload Discovery request (C-type 45)

Egress nickname (2 octets): nickname of the Egress Rbridge provided by user (used as Egress Rbridge nickname for payload generation).

Originator nickname (2 octets): nickname of the originator Rbridge.

Ingress nickname (2 octets): nickname of the ingress Rbridge.

Requester nickname (2octets): nickname of the Rbridge sending this request (Used as Ingress nickname for payload generation).

5.1.3. Pro-active Payload discovery response

'Payload generation response for Proactive monitoring' specifies one or more Destination MAC addresses, one for each ECMP. Its uses new C-type 46 which lists down destination mac addresses (DMAC1, DMAC2..DMACn where n is number of ECMPs). TRILL OAM code is set to payload generation response (23).

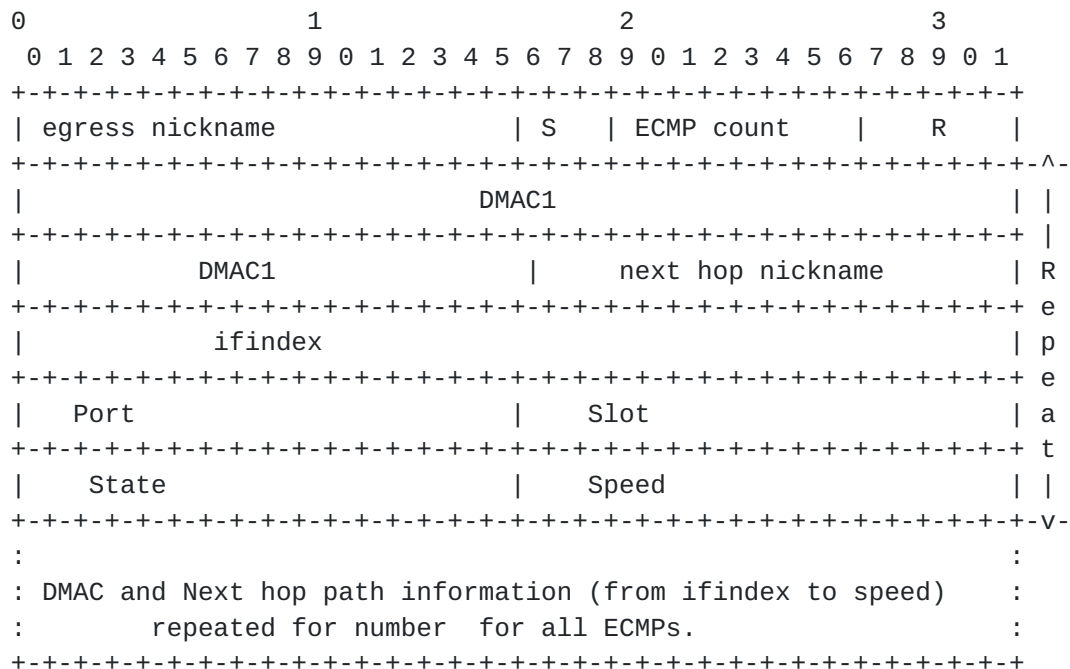


Figure 7 Pro-active Payload Discovery Response(C-type 46)

Egress nickname (2 octets): nickname of the Egress Rbridge.

S (3 bits) : indicates the status

- 0. Success
- 1. ECMP data not found
- 2. System overloaded try later
- 3. -7 Reserved MUST not be used

ECMP count(8bit) - specifies number of ECMPs

DMAC1- DMACn - Destination mac addresses, (number of MAC addresses is equal to number if ECMP count).

Next hop nickname (2 octets): nickname of the next hop Rbridge, to which packet will be forwarded if Destination mac given with this field is used.

Ifindex (4 octets) : unsigned integer of local significance

Slot (2 octets) : Slot number

Port (2 octets) : Port number

Speed (2 octets) : Speed in 100Mbps. Zero (0) indicates port speeds less than 100Mbps.

State (2 octets) : Represent the state of the port.

0: Down - no errors

1: Disable

2: Forwarding-no errors

3: Down - errors

4: Forwarding - errors

5: Forwarding - oversubscribed

6: Link monitoring disable

All other values reserved.

Total number of DMAC and next hop path information entries MUST be equal to ECMP count.

5.1.4. Pro-active fault notification

Fault details are sent to the originator Rbridge provided in the 'proactive monitoring request' by including C-type 47 (downstream identification for pro-active monitoring).

C type 47 gives information about interface on which connectivity test failed, i.e, hop count expiry message was not received.

If 'payload discovery generation response', had succeeded, one more copy of C_type 47 is included in the pro-active fault notification. The fields in this entry, are copied from the 'payload discovery generation response'. If connectivity was being tested using DMAC3 (DMAC provided in the 3rd entry in payload discovery response), the

details of the interface provided with the DMAC3 will be used in this instance of C type 47.

The notification can be sent either inband or out of band. TRILL OAM code is set to parameter problem notification (5).

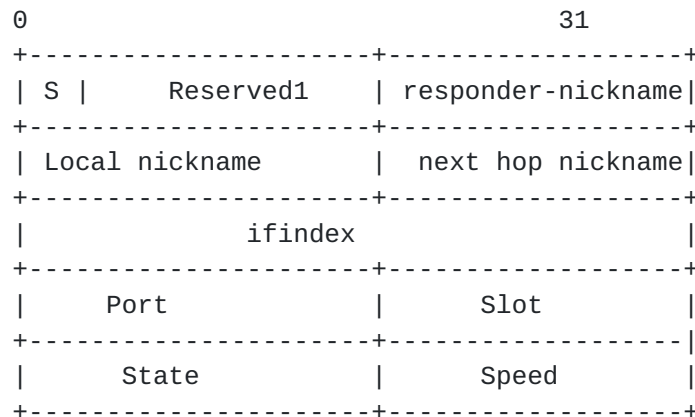


Figure 8 downstream identification for pro-active monitoring (C-type 47)

Responder nickname (16 bits): TRILL 16 bit nickname of responder RBridge [RFCtrill]

S (3 bits): 'Payload discover generation response' status from [section 5.1.3](#). If Status is not Success, remaining fields below can be set to 0.

- 0. Success
- 1. ECMP data not found
- 2. System overloaded try later
- 3. Not available
- 4. 4-7 Reserved MUST not be used

ECMP count (8 bits): Copied from for 'payload generation response', if Status was 'Success'.

Reserved1 (13 bits): Reserved, set to zero on transmission and ignored on receipt.

Next-hop neighbor information:

Local Nickname (16 bits): TRILL 16 bit nickname of the local RBridge [RFCtrill]

Next hop Nickname (16 bits): TRILL 16 bit nickname of the next hop RBridge[RFCtrill]

Slot (2 octets) : Slot number

Port (2 octets) : Port number

Speed (2 octets) : Speed in 100Mbps. Zero (0) indicates port speeds less than 100Mbps.

State (2 octets) : Represent the state of the port.

0: Down - no errors

1: Disable

2: Forwarding-no errors

3: Down - errors

4: Forwarding - errors

5: Forwarding - oversubscribed

6: Link monitoring disable

All other values reserved.

st 1 instance of C-type 47 gives information about interface connecting local Rbridge and 1st hop Rbridges.

If 'payload generation response' status ([section 5.1.3](#)), was SUCCESS, one more instance of C-type 47 is also included as part of 'pro-active fault notification.

2nd instance of C-type 47 gives information about interface connecting 1st hop Rbridge and 2nd hop Rbridges, that 'loopback message' (TRILLOAM) message would have encountered, if connectivity test was successful (i.e if hop count expiry message was received from 2nd hop Rbrige).

If 'loopback message' message (TRILLOAM) used Destination Mac address provided in the nth entry of 'payload generation response' ([section 5.1.3](#)), 2nd instance of Ctype 47 will include interface

information provided in that particular entry. In this instance of C-type 47, Status is set to 3 (not available).

6. Formal Syntax

INFO (REMOVE): Include this section only if needed. Commonly used grammar is BNF grammar defined in [RFC-2234](#). Suggested wording.

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in [RFC-2234](#) [[RFC2234](#)].

<Define your formal syntax here.>

7. Security Considerations

INFO (REMOVE): Every draft MUST have a Security Considerations section.

Security consideration for pro-active monitoring are similar to TRILL OAM draft [[TRILLOAM](#)]. Request/response packet can not go out of the TRILL cloud, as TRILL OAM ethtype packets are dropped at the Edge Rbridge. Since Pro-active monitoring request can be issued only at a TRILL Rbridge, consideration is needed only for ensuring packet with TRILL OAM ethtype and c-type 43 is dropped at Ingress Rbridge.

8. IANA Considerations

INFO (REMOVE): Every draft MUST have an IANA Considerations section, although it may be removed prior to publication by the RFC Editor if null.

<Add any IANA considerations>

9. Conclusions

<Add any conclusions>

10. References

INFO (REMOVE): Authors can use either the auto-numbered references OR the named references; typically, these would not be mixed in a single document. This template includes both examples for illustration of the two variations. Named references are preferred (e.g., [[RFC2119](#)] or [[Fab1999](#)]).

10.1. Normative References

INFO (REMOVE): Normative refs are references to standards documents ****required**** to understand this doc. These are usually Standards-track and BCP RFCs, or external (IEEE, ANSI, etc.) standards, but may include other publications.

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2234] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", [RFC 2234](#), Internet Mail Consortium and Demon Internet Ltd., November 1997.
- [RFC6325] Perlman, R. et.al. "Routing Bridges (RBridges): Base Protocol Specification", [RFC 6325](#), July 2011.
- [RFC6326] Eastlake, Donald. et.al. "Transparent Interconnection of Lots of Links (TRILL) Use of IS-IS", [RFC 6326](#), July 2011.
- [RFC4884] Bonica, R. et.al "Extended ICMP to support Multi-Part messages",[RFC 4884](#), April, 2007.
- [TRILLOAM] Senevirathne, T. et.al., "ICMP based OAM solution for TRILL", work in progress, January 2012.

10.2. Informative References

INFO (REMOVE): Informative refs are those that are not standards or standards not required to understand this doc. These are usually informative RFCs, internet-drafts (avoid if possible), and other external documents.

- [RFC792] Postel, J. "Internet Control Message Protocol (ICMP)", [RFC 792](#), September, 1981.
- [1] Faber, T., Touch, J. and W. Yue, "The TIME-WAIT state in TCP and Its Effect on Busy Servers", Proc. Infocom 1999 pp. 1573-1583.
- [Fab1999] Faber, T., Touch, J. and W. Yue, "The TIME-WAIT state in TCP and Its Effect on Busy Servers", Proc. Infocom 1999 pp. 1573-1583.

11. Acknowledgments

<Add any acknowledgements>

INFO (REMOVE): The author of this template would appreciate if you would keep the following line in your final IDs and RFCs:

This document was prepared using 2-Word-v2.0.template.dot.

Appendix A.**Sample report**

INFO (REMOVE): Starts on a new page. These are optional.

INFO (REMOVE): Careful with headers in appendices - they won't renumber when moved in/out levels in outline mode. Only Headers 1-9 do that trick, as used in the body of the RFC!

A.1. Summary Report per monitor

Monitor Vlan:

Monitor paths to RbridgeID:

Monitor Id:

Monitoring for time: x days x hours x minutes x seconds

Total Faults reported : x faults

Faulty paths detected (RbridgeId1 to RbridgeId3)

(RbridgeId1/Interface)-> (RbridgeId2/Interface)->RbridgeId3

| | | |
|-----------|-----------|----|
| S1/eth3/2 | S2/eth4/5 | S3 |
|-----------|-----------|----|

| | | |
|-----------|-----------|----|
| S4/eth5/2 | S5/eth4/5 | S3 |
|-----------|-----------|----|

<Text>

A.2. Detail Report

Fault detection log:

2012 Jan 31 13:50:34 Fault at (S1/eth3/2,S2) "ECMP information not found" for monitor to S7, vlan 2, MonitorId 10.

2012 Jan 31 13:51:24 Fault at (S4/eth5/2,S5/eth4/5,S3) "Packet flow test failed" for monitor to S8, vlan 1, MonitorId 3.

2012 Jan 31 13:52:24 Fault at (S4/eth5/2,S5/eth4/5,S3)"Packet flow test failed" for monitor to S8, vlan 1, MonitorId 3.

A.2.1. <H2>

<Text>

A.2.1.1. <H3>

<Text>

A.2.1.1.1. <H4>

<Text>

A.2.1.1.1.1. <H5>

<Text>

A.3. C type usage is messages

| Message | Mandatory parameters | Optional parameters |
|------------------------------------|---|--|
| Proactive fault monitoring request | Version(1) Pro-active fault monitoring request details(44) | Interested vlan(4) |
| Proactive fault discovery request | Version(1) Pro-active fault discovery request (45) | Interested vlan(4) |
| Proactive fault discovery response | Version(1) Pro-active fault discovery response (46) | |
| Proactive fault notification | Version(1) Pro-active fault notification(47) | Pro-active fault notification(47) (2nd instance) |

Figure 9 Optional and mandatory C-types.

New TRILL OAM code 26: Pro-active fault monitoring request

Authors' Addresses

Rohit Watve
CISCO Systems
375 East Tasman Drive,
San Jose, CA 95134

Phone: 408-424-2091
Email: rwatve@cisco.com

Tissa Senevirathne
CISCO Systems
375 East Tasman Drive,
San Jose, CA 95134

Phone: 408-853-2291
Email: tsenevir@cisco.com

Chandan Mishra
CISCO Systems
375 East Tasman Drive,
San Jose, CA 95134

Phone: 408-526-5376
Email: cmishra@cisco.com

Gayatri Ramachandran
5470 Great America Parkway,
Santa Clara, CA 95054
Phone:(408) 547-5946
Email: gayatri@aristanetworks.com