Internet Draft
Document: draft-allan-nadeau-mpls-oam-frmwk-00.txt
Category: Informational
Expires: March 2005

David Allan, Editor
Thomas D. Nadeau, Editor

September 2004

A Framework for MPLS Operations and Management (OAM)

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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 a "work in progress."

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

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

Copyright Notice

Abstract

This document is a framework for how data plane OAM functions can be applied to operations and maintenance procedures. The document is structured to outline how OAM functionality can be used to assist in fault management, configuration, accounting, performance management and security, commonly known by the acronym FCAPS.

Table of Contents

1. Introduction and Scope 2
2. Terminology.....2
3. Fault Management.....2
3.1 Fault detection.....2
3.1.1 Enumeration and detection of types of data plane faults.....3
3.1.2 Timeliness.....5
3.2 Diagnosis.....5
3.2.1 Characterization.....5
3.2.2 Isolation.....5
3.3 Availability.....5
4. Configuration Management.....5
5. Administration.....6
6. Performance measurement.....6
7. Security.....6
8. Full Copyright Statement.....7
9. Intellectual Property Rights Notices.....7
10. References.....7
11. Editors Address.....8

1. Introduction and Scope

This memo outlines in broader terms how data plane OAM functionality can assist in meeting the operations and management (OAM) requirements outlined in [REQ] and can apply to the operational functions of fault, configuration, accounting, performance and security (commonly known as FCAPS). The approach of the document is to outline the requisite functionality, the potential mechanisms to provide the function and the applicability of data plane OAM functions.

2. Terminology

OAM	Operations and Management
FCAPS	Fault, Administration, Configuration, Provisioning, and Security
ILM	Incoming Label Map
NHLFE	Next Hop Label Forwarding Entry
MIB	Management Information Base
LSR	Label Switching Router
RTT	Round Trip Time

3. Fault Management

3.1 Fault detection

Fault detection encompasses identifying all causes of failure to transfer information between the ingress and egress of an LSP

ingress. This section will enumerate common failure scenarios and explain how one might (or might not) detect the situation.

3.1.1 Enumeration and detection of types of data plane faults

Physical layer faults:

Lower layer faults are those that impact the physical layer or link layer that transports MPLS between adjacent LSRs. Some physical links (such as SONET/SDH) may have link layer OAM functionality and detect and notify the LSR of link layer faults directly. Some physical links (such as Ethernet) may not have this capability and require MPLS or IP layer heartbeats to detect failures. However, once detected, reaction to these fault notifications is often the same as those described in the first case.

Node failures:

Node failures are those that impact the forwarding capability of an entire node, including its entire set of links. This can be due to component failure, power outage, or reset of control processor in an LSR employing a distributed architecture, etc.

MPLS LSP misbranching:

Misbranching occurs when there is a loss of synchronization between the data and the control planes. This can occur due to hardware failure, software failure or configuration problems. It will manifest itself in one of two forms:

- packets belonging to a particular LSP are cross connected into a an NHLFE for which there is no corresponding ILM at the next downstream LSR. This can occur in cases where the NHLFE entry is corrupted. Therefore the packet arrives at the next LSR with a top label value for which the LSR has no corresponding forwarding information, and is typically dropped. This is a No Incoming Label Map (ILM) condition and can be detected directly by the downstream LSR which receives the incorrectly labeled packet.

- packets belonging to a particular LSP are cross connected into an incorrect NHLFE entry for which there is a corresponding ILM at the next downstream LSR, but which was is associated with a different LSP. This may be detected by a number of means:
  - o some or all of the misdirected traffic is not routable at the egress node.
  - o Or OAM probing is able to detect the fault by detecting the inconsistency between the path and the control plane.

Discontinuities in the MPLS Encapsulation

The forwarding path of the FEC carried by an LSP may transit nodes for which MPLS is not configured. This may result in a number of behaviors (most undesirable). When there was only one label in the stack and the payload was IP, IP forwarding will direct the packet to the correct interface. This would be the same if PHP is employed. Packets with a label stack will be discarded (Tom: can you confirm this for your end).

MTU problems

MTU problems occur when client traffic cannot be fragmented by intermediate LSRs, and is dropped somewhere along the path of the LSP. MTU problems should appear as a discrepancy in the traffic count between the set of ingresses and the egresses for a FEC and will appear in the corresponding MIB performance tables in the transit LSRs as discarded packets.

TTL Mishandling

Some Penultimate hop LSRs may consistently process TTL expiry and propagation at penultimate hop LSRs. In these cases, it is possible for tools that rely on consistent processing to fail.

Congestion

Congestion occurs when the offered load on any interface exceeds the link capacity for sufficient time that the interface buffering is exhausted. Congestion problems will appear as a discrepancy in the traffic count between the set of ingresses and the egresses for a FEC and will appear in the MIB performance tables in the transit LSRs as discarded packets.

Misordering

Misordering of LSP traffic occurs when incorrect or inappropriate load sharing is implemented within an MPLS network. Load sharing typically takes place when equal cost

paths exist between the ingress and egress of an LSP. In these cases, traffic is split among these equal cost paths using a variety of algorithms. One such algorithm relies on splitting traffic between each path on a per-packet basis. When this is done, it is possible for some packets along the path to be delayed due to congestion or slower links, which may result in packets being received out of order at the egress. Detection and remedy of this situation may be left up to client applications that use the LSPs. For instance, TCP is capable of re-ordering packets belonging to a specific flow. Detection of mis-ordering can also be determined by sending probe traffic along the path and verifying that all probe traffic is indeed received in the order it was transmitted.

LSRs do not normally implement mechanisms to detect misordering of flows.

Payload Corruption

Payload corruption may occur and be undetectable by LSRs. Such errors are typically detected by client payload integrity mechanisms.

3.1.2 Timeliness

(for a future version)

3.2 Diagnosis

3.2.1 Characterization

Characterization is defined as determining the forwarding path of a packet (which may not be necessarily known). Characterization may be performed on a working path through the network. This is done for example, to determine ECMP paths, the MTU of a path, or simply to know the path occupied by a specific FEC. Characterization will be able to leverage mechanisms used for isolation.

3.2.2 Isolation

Isolation of a fault can occur in two forms. In the first case, the local failure is detected, and the node where the failure occurred is capable of issuing an alarm for such an event. The node should attempt to withdraw the defective resources and/or rectify the situation prior to raising an alarm. Active data plane OAM mechanisms may also detect the failure conditions remotely and issue their own alarms if the situation is not rectified quickly enough.

In the second case, the fault has not been detected locally. In this

case, the local node cannot raise an alarm, nor can it be expected to rectify the situation. In this case, the failure may be detected remotely via data plane OAM. This mechanism should also be able to determine the location of the fault, perhaps on the basis of limited information such as a customer complaint. This mechanism may also be able to automatically remove the defective resources from and the network and restore service, but should at least provide a network operator with enough information by which they can perform this operation. Given that detection of faults is desired to happen as quickly as possible, tools which posses the ability to incrementally test LSP health should be used to uncover faults.

3.3 Availability

Availability is the measure of the percentage of time that a service is operating within specification.

MPLS has several forwarding modes (depending on the control plane used). As such more than one availability models may be defined.

4. Configuration Management

Data plane OAM can assist in configuration management by providing the ability to verify configuration of an LSP or of applications

that may utilize that LSP. This would be an ad-hoc data plane probe that should both verify path integrity (a complete path exists) as well as verifying that the path function is synchronized with the control plane. The probe would carry as part of the payload relevant control plane information that the receiver would be able to compare with the local control plane configuration.

5. Accounting

Ed Note: (for a future version)

6. Performance measurement

Performance measurement permits the information transfer characteristics of LSPs to be measured. This falls into two categories, latency and information loss.

Latency can be measured in two ways: one is to have precisely synchronized clocks at the ingress and egress such that timestamps in PDUs flowing from the ingress to the egress can be compared. The other is to use an exchange of PING type PDUs that gives a round trip time (RTT) measurement, and an estimate of the one way latency

can be inferred with some loss of precision. Use of load spreading techniques such as ECMP mean that any individual RTT measurement is only representative of the typical RTT for a FEC.

To measure information loss, a common practice is to periodically read ingress and egress counters (i.e.: MIB module counters). This information may also be used for offline correlation. Another common practice is to send explicit probe traffic. This probe traffic can also be used to measure jitter and delay.

7. Security

Support for intra-provider data plane OAM messaging does not introduce any new security concerns to the MPLS architecture. Though it does actually address some that already exist, i.e. through rigorous defect handling operator's can offer their customers a greater degree of integrity protection that their traffic will not be misdelivered (for example by being able to detect leaking LSP traffic from a VPN).

Support for inter-provider data plane OAM messaging introduces a number of security concerns as by definition, portions of LSPs will not be in trusted space, the provider has no control over who may inject traffic into the LSP. This creates opportunity for malicious or poorly behaved users to disrupt network operations. Attempts to introduce filtering on target LSP OAM flows may be problematic if flows are not visible to intermediate LSRs. However it may be possible to interdict flows on the return path between providers (as faithfulness to the forwarding path is not a return path requirement) to mitigate aspects of this vulnerability.

OAM tools may permit unauthorized or malicious users to extract significant amounts of information about network configuration. This would be especially true of IP based tools as in many network configurations, MPLS does not typically extend to untrusted hosts, but IP does. For example, TTL hiding at ingress and egress LSRs will prevent external users from using TTL-based mechanisms to probe an operator's network. This suggests that tools used for problem diagnosis or which by design are capable of extracting significant amounts of information will require authentication and authorization of the originator. This may impact the scalability of such tools when employed for monitoring instead of diagnosis.

8. Full Copyright Statement

9. Intellectual Property Rights Notices.

By submitting this Internet-Draft, the authors certify that any applicable patent or other IPR claims of which they are aware have been disclosed, or will be disclosed, and any of which they become aware will be disclosed, in accordance with RFC 3668.

10. References

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[ALLAN] Allan, D., "Guidelines for MPLS Load Balancing", draft-allan-mpls-loadbal-05.txt, IETF work in progress, October 2003

[MPLSREQS] Nadeau et.al., "OAM Requirements for MPLS Networks", draft-ietf-mpls-oam-requirements-01.txt, June 2003

[Y1710] ITU-T Recommendation Y.1710(2002), "Requirements for OAM Functionality for MPLS Networks"

11. Editors Address

David Allan
Nortel Networks Phone: +1-613-763-6362
3500 Carling Ave. Email: dallan@nortelnetworks.com
Ottawa, Ontario, CANADA

Thomas D. Nadeau
Cisco Systems Phone: +1-978-936-1470

300 Beaver Brook Drive
Boxborough, MA 01824

Email: tnadeau@cisco.com